IJCSIS Vol. 12 No. 5, May 2014
ISSN 1947-5500

International Journal of Computer Science & Information Security


Cornell University
Library


Cogprints


Google scholar


.docstoc
find and share professional documents


ScientificCommons

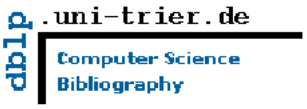

View my documents on
Scribd


BASE
Bielefeld Academic Search Engine


SCIRUS
search engine for science


SciRate.com


CiteSeerx beta


dblp .uni-trier.de
Computer Science
Bibliography


Q·Sensei


DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS


EBSCO
HOST


ProQuest

IJCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS
International Journal of Computer Science and Information Security (IJCSIS)
January-December 2014 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.
See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Scopus Database, Cornell University Library, ScientificCommons, ProQuest, EBSCO and more.

Deadline: see web site
Notification: see web site
Revision: see web site
Publication: see web site

Context-aware systems
Networking technologies
Security in network, systems, and applications
Evolutionary computation
Industrial systems
Evolutionary computation
Autonomic and autonomous systems
Bio-technologies
Knowledge data systems
Mobile and distance education
Intelligent techniques, logics and systems
Knowledge processing
Information technologies
Internet and web technologies
Digital information processing
Cognitive science and knowledge
Agent-based systems
Mobility and multimedia systems
Systems performance
Networking and telecommunications
Software development and deployment
Knowledge virtualization
Systems and networks on the chip
Knowledge for global defense
Information Systems [IS]
IPv6 Today - Technology and deployment
Modeling
Software Engineering
Optimization
Complexity
Natural Language Processing
Speech Synthesis
Data Mining

For more topics, please see web site https://sites.google.com/site/ijcsis/

For more information, please visit the journal website (https://sites.google.com/site/ijcsis/)

Editorial
Message from Managing Editor

*The **International Journal of Computer Science and Information Security** (IJCSIS) publishes carefully refereed research, review and survey papers which offer a significant contribution to the computer science literature, and which are of interest to a wide audience. Coverage extends to all main-stream branches of computer science, security and related technology applications. As a scholarly open access peer-reviewed journal, IJCSIS mission is to provide an outlet for quality research. It aims to promote universal access with equal opportunities for international scientific community; to scientific knowledge, and the creation, and dissemination of scientific and technical information.*

IJCSIS archives all publications in major academic/scientific databases. Indexed by the following International agencies and institutions: Google Scholar, Bielefeld Academic Search Engine (BASE), CiteSeerX, SCIRUS, Cornell's University Library EI, Scopus, DBLP, DOI, ProQuest, EBSCO. Google Scholar reported increased in number cited papers published in IJCSIS. Abstracting/indexing, editorial board and other important information are available online on homepage. This journal supports the Open Access policy of distribution of published manuscripts, ensuring "free availability on the public Internet, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of [published] articles".

*IJCSIS editorial board, consisting of international experts, ensures a rigorous peer-reviewing process. We look forward to your collaboration. For further questions please do not hesitate to contact us at **ijcsiseditor@gmail.com**.*

A complete list of journals can be found at:
http://sites.google.com/site/ijcsis/

IJCSIS Vol. 12, No. 5, May 2014 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

IJCSIS EDITORIAL BOARD

TABLE OF CONTENTS

Systems) organization reflects the characteristics of ocean. This is forwarded to the OIDS (Ocean Information Data System). For the data received from OIDS, pre-processing techniques are applied. Pre-processing involves the header retrieval and data separation. Header information is used to identify the region of sensor, whereas data is used in the analysis process of Ocean Information System. Analyzed data is segmented based on the region, by the header value. Mining technique and composition principle is applied on the segments for further analysis.

Index Terms-- Service oriented architecture; Text Mining; ARGO floating sensor; INCOIS; OIDS; Pre-processing.

4. Paper 30041444: DNA Sequence Alignment using Hadoop in Cloud Computing Environment (pp. 19-22)

Hamoud Alshammari, Department of Computer Science and Engineering, 221 University Ave, University of Bridgeport, Bridgeport, CT, USA

Abstract — Sequence Alignment process in DNA datasets faces different concerns, one of them is the complexity of finding any sequence since the data is unstructured and unrelated. Hadoop solves some of these issues by dividing the data into many blocks and manipulates these data perfectly with high efficient process. However, applying Hadoop has to be more accurate because DNA still needs more reliable and efficient solution because some problems might be not reliable via using Hadoop. In this project, I will explain until what extend Hadoop can solve the DNA sequence alignment with high degree of reliability.

Keywords — Cloud Computing, DNA Sequence Alignment, Hadoop, MapReduce.

5. Paper 30041445: Video Game User Interface Development Using Scaleform Gfx (CLIK™ AND SCALEFORM 3Di™) (pp. 23-28)

Oluwafemi J. Ayangbekun, Department of Information Systems, Faculty of Commerce, University of Cape Town, South Africa.
Ibrahim O. Akinde, Department of Computer Science, Faculty of Information and Communication Technology, Crescent University, Abeokuta, Nigeria.

Abstract — This paper explains how Scaleform Gfx technology can be used to create a beautifully rendered Front-End Menu using Flash Professional's proprietary language, ActionScript, both in 2D and 3D for video game development. Scaleform Gfx is cutting edge technology designed by Autodesk for creating stunning user interfaces. This paper introduces Scaleform Gfx as videogame middleware, reviews some of the previous games' user interfaces designed with Scaleform Gfx, provides an iteration of steps that can serve as a framework for creating a fully functional front-end menu and discusses the limitations of Scaleform Gfx. Also, this paper introduces Scaleform CLIK and Scaleform 3Di and explains how interoperable they are with each other when developing a user interface.

6. Paper 30041441: Bovines Muzzle Identification Using Box-Counting (pp. 29-34)

Hazem M. El-Bakry, Department of Information Systems, Faculty of Computer and Information Sciences, Mansoura University, Mansoura, Egypt
Ibrahim El-Hennawy, Hamdi A. Mahmoud, Faculty of Computer Science and Information, BeniSuef University BeniSuef, Egypt
Hagar M. El Hadad, Faculty of Computer Science and Information, BeniSuef University, BeniSuef, Egypt

Abstract — Bovines identification has become widely used as essential for guarantee the safety of cattle products and assists veterinary disease supervision and control. Texture feature extraction is a key step for muzzle image processing. In this paper, we focus on bovines muzzle patterns identification as a biological texture using a method for feature extraction of Muzzle images. The proposed method has been implemented by using Box-counting Fractal Dimension. Before texture feature extraction, preprocessing operations such as histogram equalization and morphological filtering (opening and closing) have been used for increasing the contrast and remove noise of the

image. After that, fractal dimension is calculated as the texture feature. The experimental results show that feature vector for different image of the same muzzle are highly symmetry. Therefore, it can be applied in registration of bovines for breeding and marketing systems.

Keywords-component; bovine's identification, image processing, fractal dimension, feature extraction, Box-counting

7. Paper 30041446: Electricity Power Theft Detection Using Wireless Prepaid Meter (pp. 35-78)

Ebole Alpha F., Department of Computer science, Lagos state polytechnic, Ikorodu Lagos, Nigeria
Prof: N. Goga, Department of Computer Science / Information Technology, University of Groningen, The Netherland

Abstract - Energy meters in Nigeria have dominantly been electromechanical in nature but are gradually being replaced by more sophisticated and accurate digital and electronic meters. Today, a high percentage of electricity revenue is lost to power theft, incorrect meter reading and billing, and reluctance of consumers towards paying electricity bills on time based on postpaid meter. Considerable amount of revenue losses can be reduced by using Prepaid Energy Meters. A prepaid energy meter enables power utilities to collect energy bills from the consumers prior to the usage of power by delivering only as much as what has been paid for. This research provides a prepaid energy meter behaving like a prepaid mobile phone. The meter contains a prepaid card similar to mobile SIM card. The prepaid card communicates with the power utility using mobile communication infrastructure. Once the prepaid card is out of balance, the consumer load is disconnected from the utility supply by the contactor. The power utility can recharge the prepaid card remotely through mobile communication based on customer requests or consumer purchasing recharge card. A prior billing is bound to do away with the problems of unpaid bills and human error in meter readings, thereby ensuring justified revenue for the utility. Over the past several years, smart cards have achieved a growing acceptance as a powerful tool for security, identification, and authorization. The increasing computational power placed on the chip along with advances in cryptography has made the smart card a very powerful tool for identification. The advent of multi-application smart card operating systems for both contact and contact less applications has put smart cards on the edge of information technology. The proposed system uses an IP-based controller for the prepaid meter and the load meter and the responsibility of Load meter is to provide a simple way of detecting electricity power theft without any human intervention. The Load meter would indicate exact building or location and distribution line on which unauthorized taping is done in real time. It would be time saving if distribution company personnel take reading by this wireless technique and also it would provide a digital record in case of any judicial dispute which will be use for comparative analysis between the prepaid meter. The idea is to maximize the profit margin of power utility company, efficient online control of the total amount of electricity consumed in a specific location and be able to detect when there is bypass by the user either by shoot-hunting without connecting the cable through the digital meter or parts of the equipment are connected through to the smart meter why high voltage equipment are bypassed.

Keywords: Prepaid Meter, IP-Based Controller, Load Meter.

An Advanced Bottom Up Generalization Approach For Big Data On Cloud

K.R.Pandi Lakshmi, Mphil Research Scholar,
Department of computer science,
Vel's University,
Chennai, India.

Dr.G.Rasitha Banu, Professor,
Department of Computer Science,
Vel's University,
Chennai, India.

***Abstract*— At present, the scale of data in many cloud applications increases tremendously in accordance with the Big Data trend, thereby making it a challenge for commonly used software tools to capture, manage and process such large-scale data within a tolerable elapsed time. In big data applications, data privacy is one of the most concerned issues because processing large-scale privacy-sensitive data sets often requires computation power provided by public cloud services. As a result is challenge for existing anonymization approaches to achieve privacy preservation on privacy-sensitive large-scale data sets due to their insufficiency of scalability. In this paper we propose a scalable Advanced Bottom up generalization approach for data anonymization based on Map Reduce on cloud. To make full use of the parallel capability of Map Reduce on cloud, specializations are required in an anonymization process. Original datasets are split up into a group of smaller datasets, and these datasets are anonymized in parallel, producing intermediate results. Then, the intermediate results are merged into one, and further anonymized to achieve consistent k-anonymous data sets. A group of MapReduce jobs are deliberately designed and coordinated to perform specializations on data sets collaboratively.**

Keywords- cloud; Data Anonymization; MapReduce; Bottom Up Generalization.

I. INTRODUCTION

Big data is a popular term used to describe the exponential growth and availability of data, both structured and unstructured. Big data is the term of datasets so large and complex that it becomes difficult to process using hand database management tools or traditional data processing applications. Big Data processing is performed through a programming paradigm known as MapReduce. Typically, implementation of the MapReduce paradigm requires networked attached storage and parallel processing. The fact is that with so much data being generated by so many organizations and users, storage and security simply have to become critical business issues. Ninety per cent of the total data in the world today has been created in the past two years, and 2014 and beyond will see us generating exponentially larger levels of data. So with more data comes greater threat of attack and greater need for security.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud Computing is not a very new concept in IT, in fact Cloud Computing is a more advanced version of the Data Processing Service Bureaus that we had 40 years ago. The biggest and best known Cloud Computing providers include Amazon with EC2, Microsoft with Azure and Google with Google Apps (e.g. Gmail, Google Docs, and Google Calendar). However, as the shape of the cloud computing is emerging and developing rapidly both conceptually and in reality, the legal/contractual, economic, service quality, interoperability, security and privacy issues still pose significant challenge. A task of the utmost importance is to develop a secure way for data in a hostile environment so that the published data remain practically useful while individual privacy is preserved. Cloud computing offers the promise of big data implementation to small and medium sized businesses.

Privacy is one of the most concerned issues in cloud computing, and the concern aggravates in the context of cloud computing although some privacy issues. An on-line cloud health service, aggregates data from users and shares the data with research institutes. Data privacy can be revealed with less effort by malicious cloud users or providers because of the failures of some traditional privacy protection measures on cloud. This can bring considerable economic loss or severe social reputation impairment to data owners. Hence, data privacy issues need to be addressed urgently before data sets are analyzed or shared on cloud.

We creatively apply Map Reduce on cloud to BUG for data anonymization and deliberately design a group of innovative Map Reduce jobs to concretely accomplish the generalizations in a highly scalable way. Secondly, introduce a scalable Advanced BUG approach, which performs generalization on different partitioned data set and the resulting intermediate anonymizations are merged to find final anonymization which is used to anoymize the original data set. Results show that our approach can significantly improve the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

scalability and efficiency of BUG for data anonymization over existing approaches.

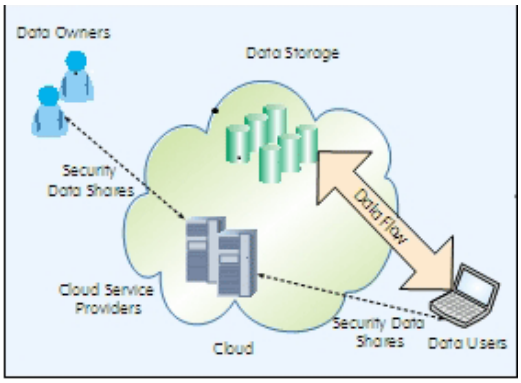


Figure 1: The Cloud System model

II. Related Work and Problem Ananlysis

A. Problem Ananlysis

A wide verity of privacy models and anonymization approaches have been put forth to preserve the privacy sensitive information in data sets. Data privacy is one of the most concerned issues because processing large-scale privacy-sensitive data sets often requires computation power provided by public cloud services for big data applications. We studied the scalability issues of existing BUG approaches when handling big data-data sets on cloud. Most exiting algorithms exploit indexing data structure to assist the process of anonymization, specifically TEA (Taxonomy Encoded Anonymity) index for BUG. TEA is a tree of m levels. The i^{th} level represents the current value for D_j. Each root to-leaf path represents a qid value in the current data table, with a (qid) stored at the leaf node. In addition, the TEA index links up the qids according to the generalizations that generalize them. The data structure TEA proposed in [239] can handle only a single QID. A new structure is required if the data holder wants to achieve LKC privacy using the Bottom-Up Generalization method because LKC privacy in effect is equivalent to breaking a single QID into multiple QIDs.

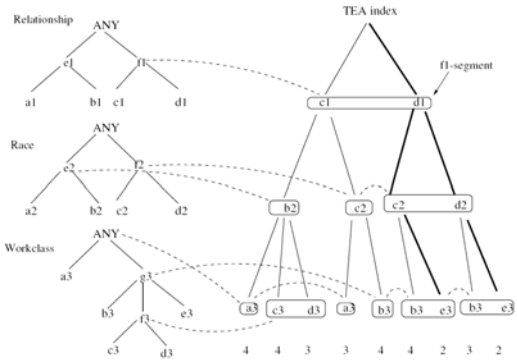


Figure 2: The TEA Structure for QID

B. Related Work

Although indexing data structures can speed up the process of data anonymization and the generalization process, because indexing structure avoids frequently scanning entire data sets and storing statistical results circumvents re-computation overheads, these approaches often fail to work in parallel or distributed environments like cloud systems because the indexing structures are centralized. There is an assumption that all data processed should fit in memory for the centralized approaches. Unfortunately, this assumption often fails to hold in most data-intensive cloud applications nowadays. Thus concluding that, the centralized approaches are difficult in handling large-scale data sets well on cloud using just one single VM even if the VM has the highest computation and storage capability. As in bottom up search strategy for finding optimization works well when the value of k is small. Centralized BUG lacks in high performance for certain value of k-anonymity parameter if they are used individually. In BUG, Calculating the ILPG and generalizing the data set involve accessing a large number of data records, thereby dominating the scalability and efficiency of Bottom-up Generalization. When generalize the information and privacy requirements to the problems of centralized anonymization and distributed anonymization, and identify the major challenges that make traditional data anonymization methods not applicable and suffer from scalable problem. MapReduce has been widely adopted in various data processing applications to push upward the scalability and efficiency. The MapReduce framework is scalable and fault-tolerant because each node in the cluster is expected to report back periodically with completed work and status updates. If a node remains silent for longer than the expected interval, a master node makes note and re-assigns the work to other nodes. As to BUG, the existing approach make full use of indexing data structure to promote efficiency, thereby falling short of high scalability and parallelization in cloud environments.

Thus, it is valuable in investigating how to develop BUG algorithm with MapReduce in order to improve the scalability and efficiency. We also attach MapReduce to improve scalability and efficiency in our research on big data anonymization. A scalable advanced Bottom-Up Generalization (BUG) approach for data anonymization based on Map Reduce on cloud will make full use of the parallel capability of Map Reduce on cloud, specializations required in an anonymization process and the scalability and efficiency of centralized BUG are improved significantly over existing approaches.

III. Methodology

Bottom-Up Generalization is an efficient k-anonymization method. In a k-anonymous data set, each record is indistinguishable from at least k−1 other records with respect to QID. Basically, Bottom-Up Generalization (BUG) approach

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

of anonymization is an iterative process starting from the lowest anonymization level. We leverage the information/privacy trade-off as the search metric for our approach, i.e., the Information Loss per Privacy Gain (ILPG). In this section we elaborate the Advanced BUG and MapReduce Bottom up Generalization (MRBUG) Driver. The Advanced BUG consists of following steps, data partition, run the MRBUG Driver on partitioned data set, combining the anonymization levels of the partitioned data set and applying generalization to original data set with integrated anonymization level without violating the k-anonymity.

A. Outline of Advanced Bottom Up Generalization

We propose an Advanced Bottom-Up Generalization (BUG) approach to improve the scalability and performance of BUG in advance fashion. The function of our approach is based on the two levels of parallelization provisioned by MapReduce on cloud. Basically, MapReduce on cloud has two levels of parallelization, i.e., job level and task level. Job level parallelization means that multiple MapReduce jobs can be executed simultaneously to make full use of cloud infrastructure resources. Task level parallelization refers to that multiple mapper/reducer tasks in a MapReduce job are executed simultaneously over data partitions. In advanced BUG, the dataset spit up is done by parallelized multi job mapreduce, and then the data set is anonymized by MapReduce Bottom up Generalization (MRBUG) Driver without violating the k-anonymity. Then all the intermediate anonymization levels are integrated, ensures that the integrated intermediate anonymized level never violates K-anonymity, the more general one is selected as the integrated one. After obtaining the merged intermediate anonymization level, we execute the driver on the entire original data set, and get the resulting anonymization level. Then, the data set is anonymized by replacing original attribute values in it with the responding domain values obtained by the resulting anonymization level. The procedure for Advanced Bottom Up Generalization is as follows.

Input: *Dataset DS, Anonymity k, k^1, partition p, record r, r DS, Anonymization Level AL_0*

Procedure:

1. *Scan DS and Generate a Random number ran,*
   Emit (ran, r)
2. *For each ran*
   Emit (null, list(r))
3. *Run MRBUG Driver with DS_i, k^1, AL^o as parameters where $1 \le i \le p$, results $AL^1{}_i$*
4. *Merge all $AL^1{}_i$ where the resulting AL^2 should general or identical.*
5. *Run MRBUG Driver with DS, k, AL^2 as parameters, results AL^**
6. *For each attribute value v_i in r, find gen in AL^**
7. *Generate $r^*=(q_1, q_2, ..., q_m)$, q is quasi-identifier, m is number of attributes*
8. *If gen is INACTIVE then emit (r^*,count)*
9. *For each r^* sum $\rightarrow \sum$ count*
10. *Emit (r^*,sum)*

B. Data Split Ups

Here the original data set *DS* is partitioned into smaller ones. Let DS_i, where $1 \le i \le p$, denote the data sets partitioned from *DS*, where *p* is the number of partitions. Specifically, a random number *ran*, where $1 \le ran \le p$, is generated for each data record. A record is assigned to the partition DS_{ran}.

Anonymization is not invulnerable counter measures that compromise current anonymization techniques can expose protected information in released datasets. After getting the partitioned data set DS_i, we run *MRBUG* (DS_i , k^1, AL^o) on these data sets in parallel to derive intermediate anonymization levels $AL^1{}_i$ where $1 \le i \le p$.

C. Integrating the Partitioned Data

Here the intermediate anonymization levels are merged into one (AL^2). The merging of anonymization levels is completed to ensure that the merged intermediate anonymization level (AL^2) never violates privacy requirements, the more general and identical one is selected as the merged one. If the intermediate anonymization levels $AL^1{}_i$ satisfies privacy requirements, then the merged anonymization level AL^2 will not violate the privacy requirements. Then, MRBUG can further anonymize the entire data sets to produce final *k*-anonymous data sets.

D. MRBUG Driver

MRBUG plays a main role in the Advanced BUG approach, as it is invoked by two times to concretely process generalization. Basically, a practical MapReduce program consists of *Map* and *Reduce* functions, and a *Driver* that coordinates the macro execution of jobs. Each round of BUG iteration includes four major steps, namely, checking the current data set whether satisfies the anonymity requirement, calculating the ILPG, finding the best generalization and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

generalizing the data set according to the selected best generalization. An existing approach uses indexing data structure but MapReduce does not support indexing data structure. So for calculating ILPG we use mapreduce jobs. The procedure for MRBUG driver is as follows.

Input: *Data Set DS, Anonymity k, Data record (ID_r, r), r DS, Anonymization Level AL_0*

Procedure:

1. *Scan DS and initialize search metric ILPG*
2. *For each(if Anonymity <k before generalization) Find gen_{best} and set it INACTIVE*
3. *if set of gen and its siblings are INACTIVE then Insert gen_{new} to replace INACTIVE ones*
4. *$AL_{i+1} \leftarrow AL_i$; Update search metric ILPG for all active gen*
5. *Repeat the iteration*

The MRBUG Driver starts by initiating the search metric values ILPG, next it checks for current anonymity satisfies the privacy requirements, the driver finds the best generalization of Highest ILPG and set gen_{best} as INACTIVE that means gen_{best} is not consider for next iteration. If set of all gen and its siblings are labeled as INACTIVE then insert new higher level generalization to replace all the INACTIVEs. At last reset new value for anonymization level and update the search metric ILPG. For initiating and updating the search metric ILPG involves accessing to the original data set and computing statistic information over the data set. The process of generalization also involves accessing to the original data set. The information loss of a generalization will not be affected when we perform other generalizations or insert a new generalization, while privacy gain will probably be impacted as the anonymity of the data set will change. The essential of computing anonymity of a data set is to find out the minimum QI-group size. The ILPG calculation results in Information gain, anonymity for generalizations and intermediate key value pair (key, count). *Map* and *Reduce*, defined over a data structure named key-value pair (*key*, *value*). *Map* takes a pair ($k1$, $v1$) as input and then outputs another intermediate key-value pair ($k2$, $v2$). These intermediate pairs are consumed by the *Reduce* function as input. Reduce takes intermediate $k2$ and all its corresponding values *list* ($v2$) as input and outputs another pair ($k3$, $v3$).

E. Data Generalization

The original data set is concretely generalized for data anonymization by a MapReduce job. The *Map* function emits anonymous records and its count according to the current anonymization level. The *Reduce* function simply aggregates these anonymous records and counts their number. An anonymous record and its count represent a QI-group, and the QI-groups constitute the final anonymous data sets.

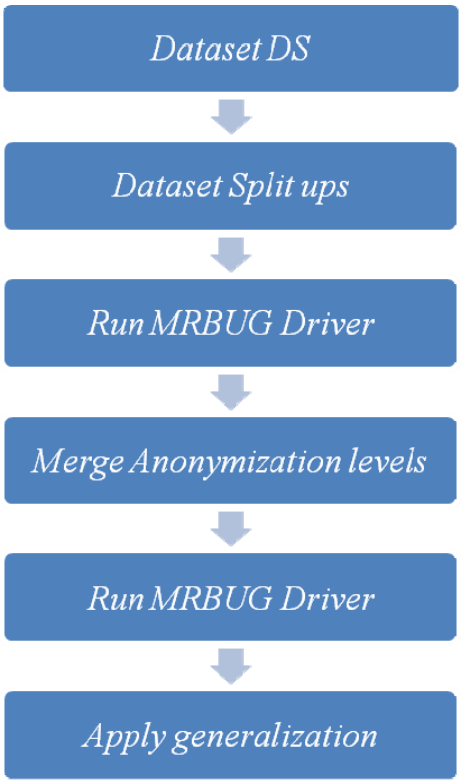


Figure 3: The Flow Diagram

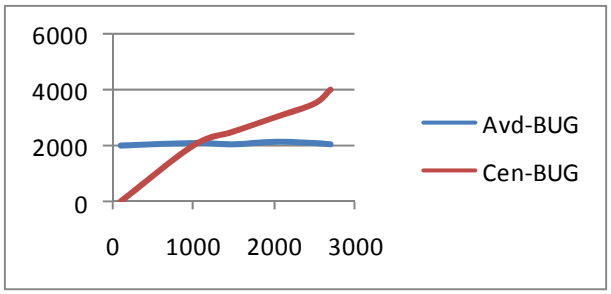
IV. SAMPLE EVALUVATION

To evaluate the effectiveness and efficiency of the Advanced BUG approach, we compare Advanced BUG with centralized BUG. We denote the execution time of the two approaches as Adv-BUG and cen-BUG, respectively. Our experiments are conducted in a cloud environment named Amazon Elastic MapReduce. Amazon Elastic MapReduce (EMR) is a web service that uses Hadoop, an open-source framework, to quickly & cost-effectively process vast amounts of data. Elastic MapReduce is a web service built on top of the Amazon cloud platform. All approaches are implemented in Java and standard Hadoop MapReduce API. We utilize the Health Care Sample data set from *US Government Open Data Projects (Dataset)*.

We measure the change of execution time Cen-BUG and Adv-BUG with respect to data size. We can see from Fig.4 that the execution time of the Advanced approach is kept under a certain level, while centralized BUG incur high execution time when the data increases in size. Hence, Cent-BUG suffers from scalability problem for large-scale data sets. The above experimental results demonstrate that our approach

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

can significantly improve the scalability and efficiency compared with Centralized approaches.



X-axis: data size in MB; Y-axis: time in seconds

Figure 3: Change of execution time with respect to data size

V. CONCLUTION

In this paper, we studied the scalability problem of data anonymization for big data applications on cloud using Bottom Up Generalization (BUG) and proposed scalable Advanced Bottom Up Generalization. The proposed BUG performed as Data partitioned, executing the driver producing intermediate results. Then, the intermediate results are merged and generalization is applied to produce anonymized data without violating *k*-anonymity. The MapReduce Framework is effectively applied on cloud for data anonymization and shows that scalability and efficiency of centralized BUG are improved significantly over existing approaches. In future optimized balanced scheduling strategies are expected to be developed towards overall scalable privacy preservation aware dataset scheduling. And also our method is designed for achieving k-anonymity; it can be modified to adopt the LKC-privacy model in order to accommodate the high-dimensional data.

ACKNOWLEDGMENT

I owe my thanks to a great many people who helped and supported me for making this paper.

I express my deep and sincere gratitude to my university for giving me a platform to exhibit my knowledge.

I extend my reverential gratitude to Dr.G.Rasitha Banu, professor, department of computer science at Vel's university for her valuable guidance and support for making this paper.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M.Zaharia, "A View of Cloud Computing," Commun. ACM, vol.53, no. 4, pp. 50-58, 2010.

[2] L. Wang, J. Zhan, W. Shi and Y. Liang, "In Cloud, Can Scientific Communities Benefit from the Economies of Scale?," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 2, pp.296-303, 2012.

[3] H. Takabi, J.B.D. Joshi and G. Ahn, "Security and Privacy Callenges in Cloud Computing Environments," IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, 2010.

[4] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Fut. Gener. Comput. Syst., vol. 28, no. 3, pp.583-592, 2011.

[5] X. Zhang, Chang Liu, S. Nepal, S. Pandey and J. Chen, "A Privacy Leakage Upper-Bound Constraint Based Approach for Cost-Effective Privacy Preserving of Intermediate Datasets in Cloud," IEEE Trans. Parallel Distrib. Syst., In Press, 2012.

[6] I. Roy, S.T.V. Setty, A. Kilzer, V. Shmatikov and E. Witchel, "Airavat: Security and Privacy for Mapreduce," Proc. 7th USENIX Conf. Networked Systems Design and Implementation (NSDI'10), pp. 297-312, 2010.

[7] T. Iwuchukwu and J.F. Naughton, "K-Anonymization as Spatial Indexing: Toward Scalable and Incremental Anonymization," Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB'07), pp. 746-757, 2007.

[8] S. Chaudhuri, "What Next?: A Half-Dozen Data Management Research Goals for Big Data and the Cloud," in Proc. 31st Symp. Principles of Database Systems (PODS'12), pp. 1-4, 2012.

[9] B.C.M. Fung, K. Wang and P.S. Yu, "Anonymizing Classification Data for Privacy Preservation," IEEE Trans. Knowl..Data Eng., vol. 19, no. 5, pp. 711-725, 2007.

[10] J. Ekanayake, H. Li, B. Zhang, T. Gunarathne, S.-H. Bae, J. Qiu and G. Fox, "Twister: A Runtime for Iterative Mapreduce,"Proc. 19th ACM Int'l Symp. High Performance Distributed Computing (HDPC'10), pp. 810-818, 2010.

[11] V. Borkar, M.J. Carey and C. Li, "Inside "Big Data Management": Ogres, Onions, or Parfaits?," Proc. 15th Int'l Conf. Extending Database Technology (EDBT'12), pp. 3-14, 2012.

[12] K. LeFevre, D.J. DeWitt and R. Ramakrishnan, "Mondrian multidimensional k-anonymity," Proc. 22nd International Conference on Data Engineering (ICDE '06), article 25, 2006.

[13] T. Li, N. Li, J. Zhang and I. Molloy, "Slicing: A new approach for privacy preserving data publishing," IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 3, pp. 561-574, 2012.

[14] N. Li, T. Li and S. Venkatasubramanian, "Closeness: A new privacy measure for data publishing," IEEE Transactions on Knowledge and Data Engineering, vol. 22, no. 7, pp. 943-956, 2010.

[15] B.C.M. Fung, K. Wang, R. Chen and P.S. Yu, "Privacypreserving data publishing: A survey of recent developments," ACM Computer Survey, vol. 42, no. 4, pp. 1-53, 2010.

[16] M. Terrovitis, J. Liagouris, N. Mamoulis and S. Skiadopolous, "Privacy preservation by disassociation," Proceedings of the VLDB Endowment, vol. 5, no. 10, pp.944-955, 2012.

[17] J. Dean and S. Ghemawat, "MapReduce: A flexible data processing tool," Communications of the ACM, vol. 53, no. 1, pp. 72-77, 2010.

[18] D. E. Denning. Commutative filters for reducing inference threats in multilevel database systems. In Proc. of the IEEE Symposium on Security and Privacy (S&P), Oakland, CA, April 1985.

[19] C. Diaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity. In Proc. of the 2nd Internationl Workshop on Privacy Enchancing Technologies (PET), pages 54–68, San Francisco, CA, April 2002.

[20] J. Goguen and J. Meseguer. Unwinding and inference control. In Proc. of the IEEE Symposium on Security and Privacy (S&P), Oakland, CA, 1984.

[21] L. Hsiao-Ying and W.G. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 995-1003, 2012.

[22] P. Mohan, A. Thakurta, E. Shi, D. Song and D. Culler, "Gupt: Privacy Preserving Data Analysis Made Easy," Proc. 2012 ACM SIGMOD Int'l Conf. Management of Data (SIGMOD'12), pp. 349- 360, 2012.

[23] Amazon Web Services, "Amazon Elastic Mapreduce," http://aws.amazon.com/elasticmapreduce/, accessed on: Jan. 05, 2013.

[24] Apache, "Hadoop," http://hadoop.apache.org, accessed on: Jan.05, 2013.

[25] Y. Bu, B. Howe, M. Balazinska and M.D. Ernst, "The Haloop Approach to Large-Scale Iterative Data Analysis," VLDB J., vol. 21, no. 2, pp. 169-190, 2012.

AUTHORS PROFILE

K.R.PANDILAKSHMI She is currently working towards the M.Phil Degree at Vel's University,chennai,India. Before joining vel's university,she has received her Master's degree in Computer Science from Bharathidasan University,India and Bachelor's degree in computer science from Kamaraj University,India. Her research interest include cloud computing, data privacy and security, Big DataMap Reduce. She has published a paper in National journal on data mining and information security.

DR.G.RASITHA BANU She is a professor in Computer Science Department, Vel's University, Chennai, India. Her Current research interest is in Data mining and Image Processing. She has Published several papers in National journal and International Journal

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Proposal of Countermeasure against Attacks Similar to Stuxnet

Youssef ZIZA
RITM LAB ESTC
CED ENSEM Hassan II University,
Casablanca, Morocco
ziza.youssef@gmail.com

Hicham BELHADAOUI
RITM LAB ESTC
Hassan II University,
Casablanca, Morocco
belhadaoui@est-uh2c.ac.ma

Nadia AFIFI
RITM LAB ESTC
Hassan II University,
Casablanca, Morocco
nafifi@est-uh2c.ac.ma

Mounir RIFI
RITM LAB ESTC
Hassan II University,
Casablanca, Morocco
rifi@est-uh2c.ac.ma

***Abstract*— A command control system refers to a general control system, of a production system, of a process, or of another type of dynamic system, wherein the control elements are not centralized, but are distributed throughout the system; and each component or sub- system is controlled by one or more controllers.**

DCS (Distributed Control System) is a computerized control system used to control the production line in the industry

The entire controller system is connected via networks communication and monitoring. DCS is a very broad term used in various industries, to monitor and control distributed equipment.

Nowadays, there are generally an information system upstream command control systems. To ensure the security of a system, we must secure the weakest link of this system. Thus, a flaw in the information system can lead to a multitude of command control system vulnerabilities.

This is considered as a real threat to the states [1] and can lead to disasters [2]. A multitude of vulnerabilities currently affects these systems. These vulnerabilities are exploited for various reasons such as cybercrime, industrial espionage or other.

The objective of our work is to analyze the workings of Stuxnet and to propose countermeasures to strengthen the security of command control systems.

***Key Words*— Stuxnet, Strong authentication, SCADA, HOTP.**

I. INTRODUCTION

Since its discovery in June 2010, the Stuxnet virus has made a lot of ink flow; not only for the sophisticated manner in which it is designed, but also because of the nature of the systems attacked, considered as critical, i.e., systems Supervisory Control And Data Acquisition (SCADA), which are essential in the industrial world.

That's why; a large number of studies on the functioning of Stuxnet were carried out. They give more details on the vulnerabilities exploited, in order to infiltrate and to spread in systems.

To better understand the attack, we will analyse the functioning of Stuxnet, which will allow us to identify gaps and different access systems; and thereafter to propose a countermeasure able to prevent this kind of attack.

In our paper, we used Boolean logic modeling Driven Markov Process (BDMP) Stuxnet which was conducted by researchers [3] to quantify and calculate the probabilities of successful attacks. This allow us to better identify risk areas for suggesting the best countermeasures

This model allow us to (i) have a disambiguation, (ii) have a better readability and conciseness, (iii) study the behavior of the system before and after implementation of countermeasures, and evaluate the added value of our solution.

Our paper is organized as follows: In Section II we present the state of the art on Stuxnet. In Section III we present the functioning of Stuxnet. Section IV is dedicated to proposed countermeasures. Section V, present a qualitative study of our proposal, and we finish with a conclusion and perspectives.

II. STATE OF THE ART

In this chapter, we describe the Stuxnet virus then we present the BDMP formalism used to modeling the Stuxnet. After, we introduce the systems attacked by this virus, and we finish by

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

presenting the methods used to protect systems with strong authentication using the HMAC ONE TIME PASSWORD established by the Open Authentication consortium.

A. Boolean logic Driven Markov Process (BDMP)

BDMP is a graphical modeling formalism originally designed for safety and reliability assessment of systems. This formalism is an extension of fault trees used to represent Markov graphs of large size . It therefore provides a good readability, a good hierarchical representation and an advanced quantification capabilities. The formalism BDMP offers, features dynamic modeling with a particular type of link called "triggers."

Fig.1 shows an example of modeling BDMP

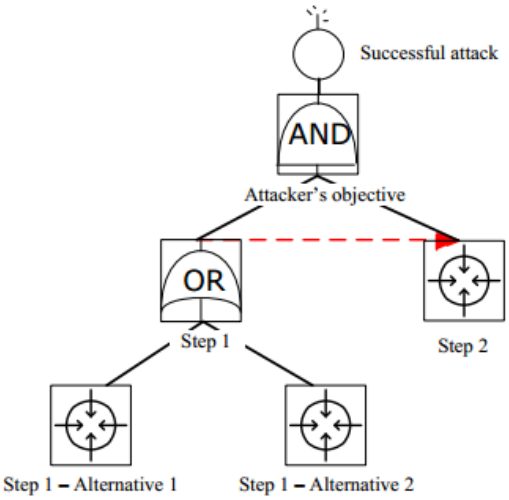


Figure 1: Modeling BDMP

B. Stuxnet virus:

Stuxnet is a virus developed to attack information systems using SCADA networks exploiting. This virus has infected thousands of machines, based on a new technique of attack. This is achieved by the use of trusted certificates, allowing it, to be executed in legitimacy in windows OS. The functioning of the virus is presented bellow.

After his appearance, many countermeasures were made, like the proposal done by Siemens WinCC SCADA System editor, who offer a tool to remove Stuxnet. Microsoft have also, corrected the vulnerabilities exploited by the virus (for possessing the administrator's rights) [9]. But the exploitation of any zero-day vulnerabilities may lead to a same result. If one of the exploited Windows vulnerabilities is not corrected, it will allow modifying the executed processes, and this is considered as a real danger.

C. Supervisory Control And Data Acquisition SCADA:

The networks SCADA is a set of computers and applications that perform key functions in the delivery of services and commodities (electricity, natural gas, etc) and offers remote management on a large scale distributed at measures and controls [5].

D. Open Authentication OATH:

It is a consortium in which there are large companies driven by the strong growth which aims to improve safety in a world increasingly connected. It provides solutions that enable strong authentication for all users on all devices and networks [6].

E. Hashed Message Authentication Code One Time Password HOTP:

HMAC OTP (HOTP) is an algorithm to generate the one-time-password value based on Hashed Message Authentication Code (HMAC) [7]. This algorithm is used in a wide variety of networks and systems application. We give an example of the implementation of this algorithm in chapter IV.

F. Dynamic Link Library DLL:

DLLs are executable files that allow applications to share code to perform one or more predefined functions. One of the biggest advantages is that a DLL is not loaded into memory, which saves memory while allowing several programs to function effectively. However, there are malicious DLL. These programs can change the parameters of the systems and allow to intruders to remotely access to these latter.

III. FUNCTIONING OF STUXNET

Generally, the machines are infected by execution of autorun.inf or by file sharing. The machines are infected by loading a DLL file. This file contain a multiple functions which are exploited later by Stuxnet, subsequently, the virus checks the machine's configuration and its environment, in order to choose the continuation or discontinuation of scripts based on the machine configuration.

If the configuration of the system is correct and updated; Stuxnet verifies if it possesses the administrator rights, if not, it exploits one of the two zero-day vulnerabilities in order to get the required rights [9]: (i) CVE- 2010-2743 (MS -10- 073) Or (ii) vulnerability in the Windows Task Scheduler.

Both vulnerabilities allow any program to have privileges, and also, to be run in a new process or as a new task in the task manager. The environment is now ready to be infected by Stuxnet. The infection process is done according to the antivirus installed.

Stuxnet installs the device drivers in the registry, to ensure their performances every time the machine started. They are loaded before all Windows applications.
Then it changes the settings of the Windows Firewall (Windows Defender) to avoid being blocked later [10]. The Fig.2 shows the different steps of that operation.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

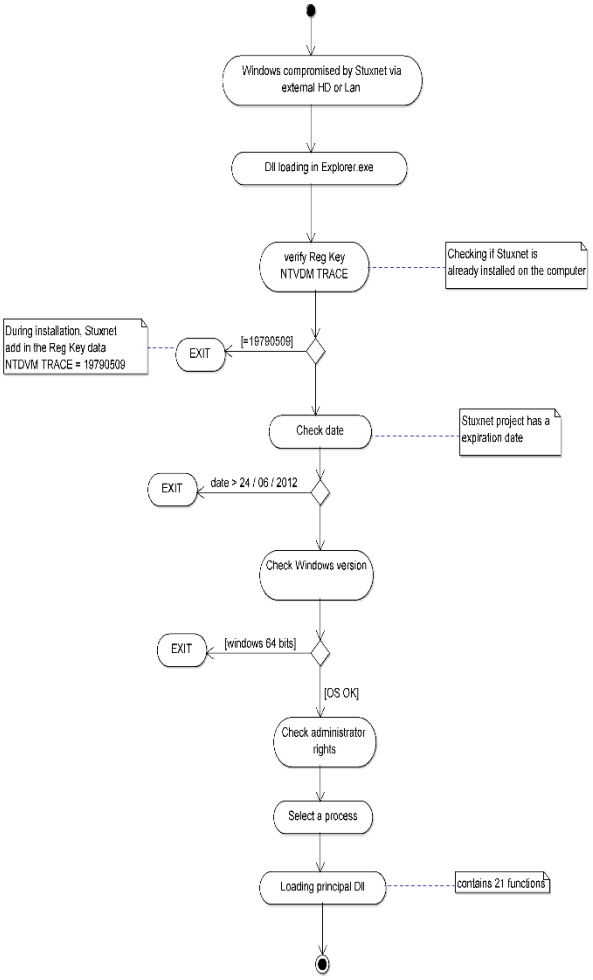


Figure 2 : STUXNET functioning Diagram

Stuxnet uses a special method to load the DLL; normally the function LoadLibrary loads the DLL from the ROM and not from RAM. But Stuxnet is able to load the DLL from RAM. This operation is possible thanks to a special method explained below.

Stuxnet is installed by loading in a process the Stuxnet modules from the explorer.exe

He overwrites the old functions that contains the process and writes its own functions, after that, it patch APIs processes modifying their names, and then writes the parameters of the new features in the MZ header.

These operations make believe that the DLL is loaded from the ROM.

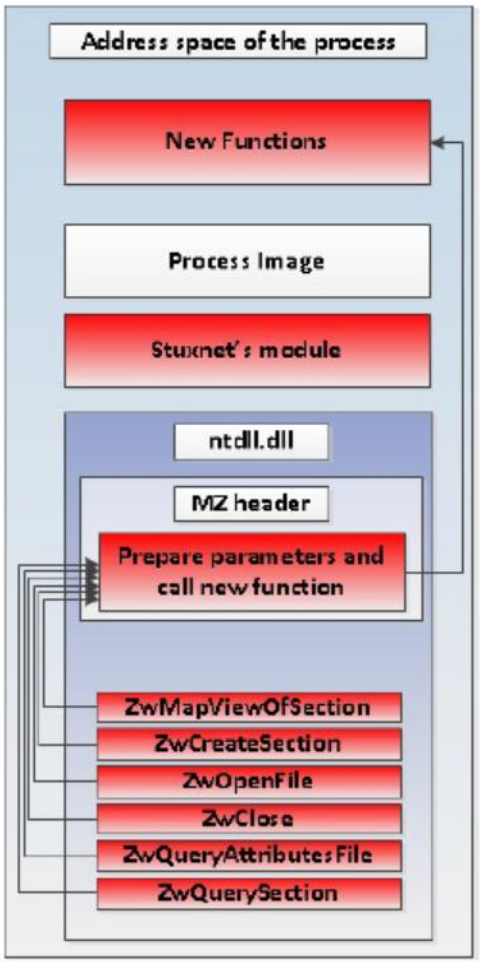


Figure 3: Hook DLL Functioning

Stuxnet is based on WriteProcessMemory or CreateRemoteThread [12] functions that write data in an area of memory in a specified process.

The Fig.4 illustrates the method used by Stuxnet to load the DLL:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

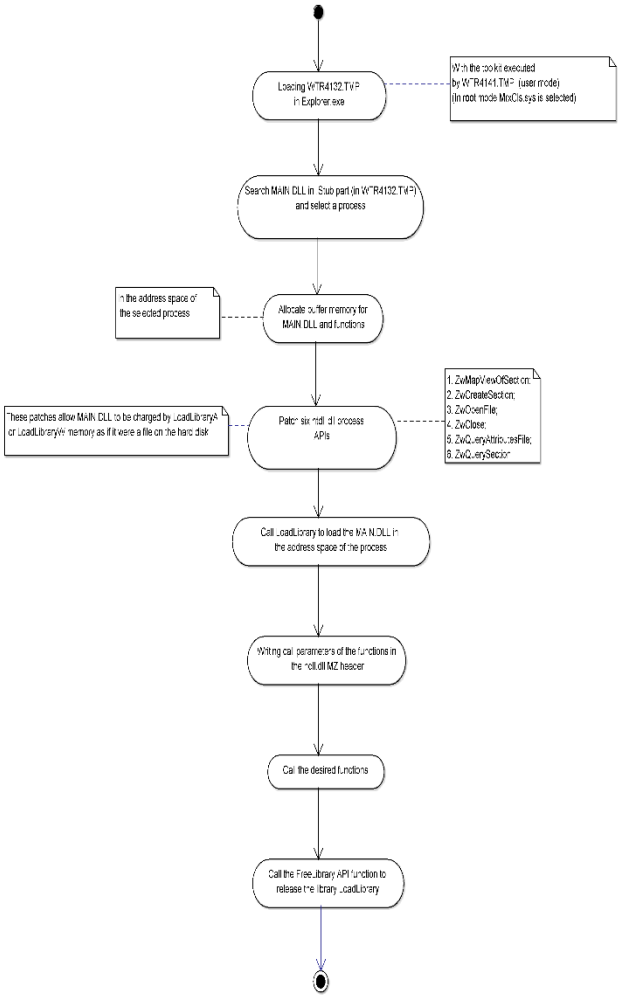


Figure 4: Stuxnet Loading DLL

One of the weaknesses of the system is the lack of verification of the entity identity which aims to change the process. thats why we propose to increase the level of security using authentication at this point.

IV. COUNTERMEASURES

We propose to use a multi-factor authentication as solution. This multi- factor authentication makes the systems more secure in case a virus exploits vulnerabilities in order to modify functions in the process already executed. The virus would not be able to use all the features of the machine if it does not have the OTP generated by the token: The use of machine resources requires a OTP for access to resources. This solution aims to secure: (i) Access to resources, (ii) Writing in files, (iii) Execution of applications (iv) Changes in the DLL.

In Fig.3 and Fig.4, we explained how Stuxnet is installed on machines, and one of the main steps that allows this installation is the exploitation of WriteProcessMemory or CreateRemoteThread; that allow to Stuxnet to write in a process running, and change the APIs.

In this paper we propose the use of the OTP whenever we want to change any process executed by the system. In this case, an OTP is requested, and only after the authentication, process may perform changes. Otherwise, the operation fails.

The diagram in Fig.5 shows at what level we can introduce the countermeasure.

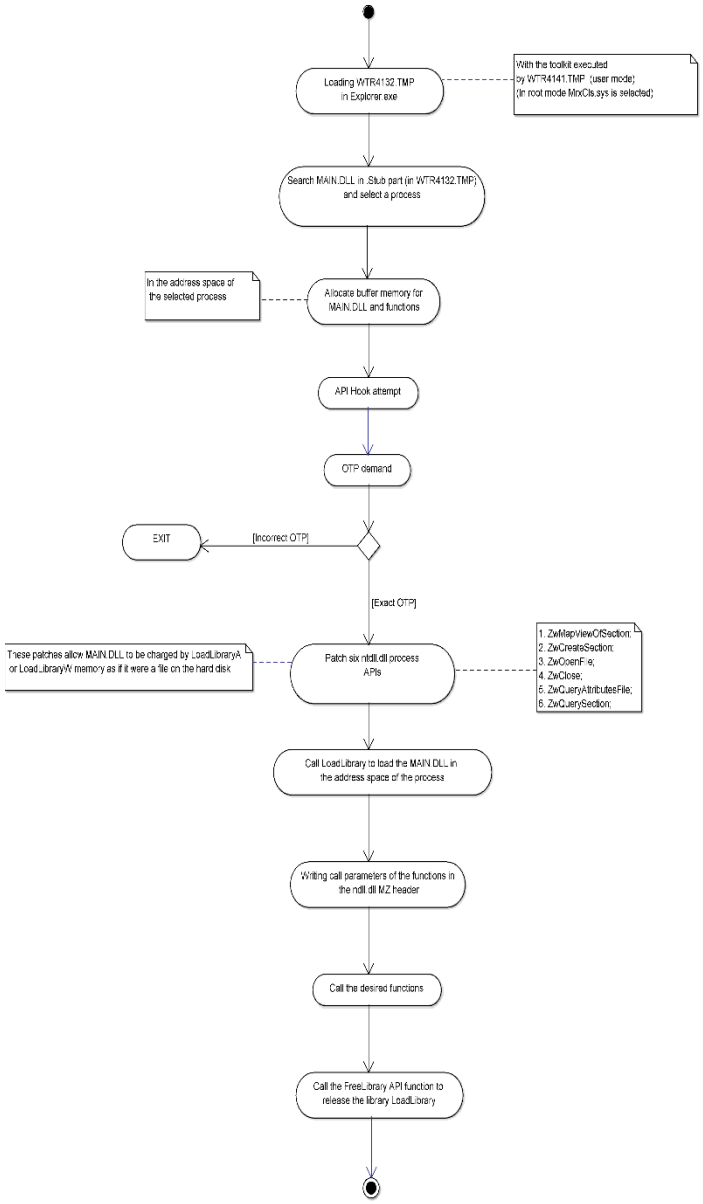


Figure 5: Loading DLL with OTP

The generation process of the HOTP is based on the algorithm defined in the RFC 4226. We have studied the behavior of Stuxnet for knowing at what level the implementation of this solution is the most effective.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

We have therefore proposed a modification of both WriteProcessMemory function and CreateRemoteThread function of windows systems.

The syntax of WriteProcessMemory function that writes data to a memory area in a specified process coded in C + + is:

```
BOOL WINAPI WriteProcessMemory(
 _In_  HANDLE hProcess,
 _In_  LPVOID lpBaseAddress,
 _In_  LPCVOID lpBuffer,
 _In_  SIZE
T nSize,
 _Out_ SIZE_T *lpNumberOfBytesWritten
);
```

We proceed to modify the function by adding an OTP authentication:

```
BOOL WINAPI WriteProcessMemory(
 _In_  HANDLE hProcess,
 _In_  LPVOID lpBaseAddress,
 _In_  LPCVOID lpBuffer,
 _In_  SIZE_T nSize,
 _In_  LPSTR hOtp,
 _Out_ SIZE_T *lpNumberOfBytesWritten
);
```

The same changes are applied on the CreateRemoteThread function:

```
HANDLE WINAPI CreateRemoteThread(
  _In_   HANDLE hProcess,
  _In_   LPSECURITY_ATTRIBUTES
lpThreadAttributes,
  _In_   SIZE_T dwStackSize,
  _In_   LPTHREAD_START_ROUTINE
lpStartAddress,
  _In_   LPVOID lpParameter,
  _In_   DWORD dwCreationFlags,
  _Out_  LPDWORD lpThreadId
);
```

Changed to:

```
HANDLE WINAPI CreateRemoteThread(
  _In_   HANDLE hProcess,
  _In_   LPSECURITY_ATTRIBUTES
lpThreadAttributes,
  _In_   SIZE_T dwStackSize,
  _In_   LPTHREAD_START_ROUTINE
lpStartAddress,
  _In_   LPVOID lpParameter,
  _In_   DWORD dwCreationFlags,
  _In_  LPSTR hOtp,
  _Out_  LPDWORD lpThreadId
);
```

In the event that the OTP is not correct, an error is triggered and stops the further modification process.

As explained in RFC 4226 [7], the HOTP is based on a incrementing counter (C) and a secret key (K) shared between the machine and the device (token). An example of the implementation of HOTP with a python code is given in Fig..

```
#!/usr/bin/env python
"""
OATH HOTP + TOTP Implementation in python.

Based on http://tools.ietf.org/html/rfc4226

Parameter and function names kept inline with the
RFC
(e.g. HOTP, Truncate, K, C etc)
"""

import hmac
import hashlib

def HOTP(K, C, digits=6):
    C_bytes = _long_to_byte_array(C)
    hmac_sha1 = hmac.new(key=K,msg=C_bytes,

digestmod=hashlib.sha1).hexdigest()
    return Truncate(hmac_sha1)[-digits:]
```

V. QUALITATIVE STUDY OF THE ESTABLISHMENT OF A OTP

We have seen in Fig.5 that the use of various system vulnerabilities allows to Stuxnet (or other type of worm exploiting the same vulnerabilities) to damage a system, especially in the context of a targeted attack. We proposed a solution based on RFC 4226. In this chapter we are going to evaluate the contribution of the proposed countermeasure, for know what our proposal brings to systems. Also, to know at what kind of security requirements it meets.

Our choice was made on the evaluation made by the method of Common Criteria [13].

Consider the case where the entities that contain SCADA systems are the Target Of Evaluation TOE. The evaluation we do concern the requirements of security, such as: availability, confidentiality and integrity. In our case the proposed countermeasure that is OTP (RFC 4226) for secure against modification in the started process, increases availability

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

because the right resource can be accessed only by the appropriate entity.

Fig.6 illustrates these high level concepts and relationships

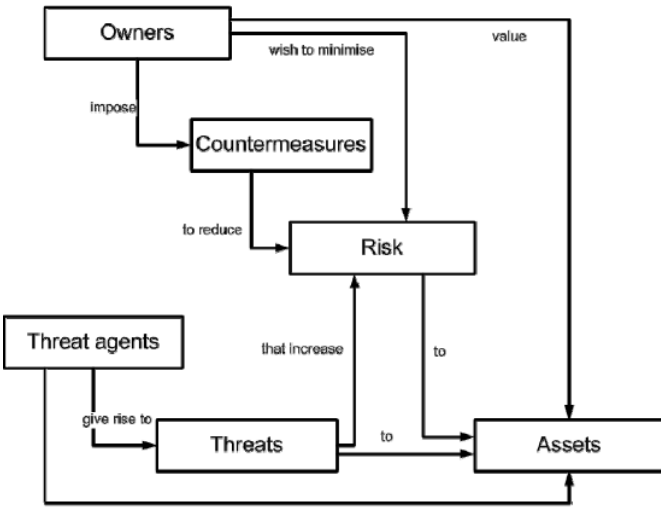


Figure 6: Security concepts and relationships

Our approach allow to have a protection profile different from the profile without OTP, which not only improves the level of system availability, but also the integrity, because the information cannot be changed only by entities entitled [14].

The Fig.7 show the method used to evaluate the countermeasures.

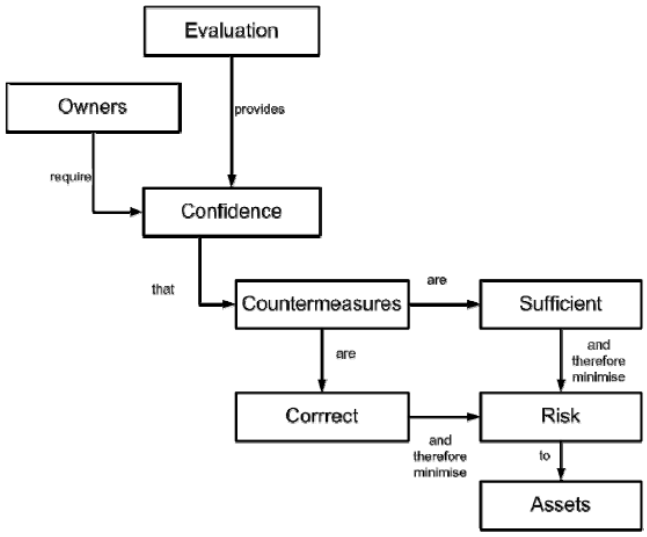


Figure 7: Evaluation concepts and relationships

The table below shows the impact of the establishment of a security solution with OTP on the various parameters of the requirements of security: confidentiality, integrity and availability.

	Disponibility	Confidentiality	Integrity
Without OTP	--	same	--
With OTP	++	same	+

Figure 8: Comparison of protection profile with and without OTP

The three criteria are different, and their improvement is ensured by different methods but the improving of one of the criteria has an impacts on the improvement of the other criteria systematically. [14].

VI. Conclusion

Viruses, as Stuxnet continue to spread, exploiting technical and humans vulnerabilities. In this paper we treated countermeasures that block any viruses based on a loading of the DLL. In future work we are going to make a quantitative study of the proposed solution. Then, we aim prepare a set of tools to detect and prevent against this type of attack

REFERENCES

[1] M. Bouissou 200 BDMP (Boolean logic Driven Markov Processes) as an alternative to Event Trees. EDF R&D, Clamart, France (paper)

[2] USA Depatement of energy 21 Steps to improve cyber security of scada networks
http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf 11P

[3] Modeling the Stuxnet Attack with BDMP: Towards More Formal Risk AssessmentsSiwar Kriaa. Grenoble Institute of Technology, Marc Bouissou École Centrale de Paris, Ludovic Piètre-Cambacédès Electricité de France (EDF) R&D (Paper)

[4] Evaluation of the impact of cyber security of command control systems. Expertise Report Project Raffaëlli Bruno 2012

[5] Cyber Security of Water SCADA Systems. Analysis and Experimentation of Stealthy Deception Attacks IEEE (paper)

[6] Initiative of open authentication 24/11/2013 http://www.openauthentication.org/aboutOath.

[7] RFC 4226 http://www.ietf.org/rfc/rfc2104.txt

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[8] Stuxnet An overview & analysis. Sam Skalicky & Biru Cui College of Computing & Information Sciences Rochester Institute of Technology (Paper)

[9] CVE http://www.securityfocus.com/bid/43774/discuss

[10] Stuxnet Under the Microscope. ESET Aleksandr Matrosov, Senior Virus Researcher Eugene Rodionov, Rootkit Analyst David Harley, Senior Research Fellow Juraj Malcho, Head of Virus Laboratory P85

[11] The Cousins of Stuxnet: Duqu, Flame, and Gauss Boldizsar Bencsath, Gàbor Pék, Levente Buttyan, and Mark Félegyhazi 6 November 2012 P1001

[12] Create remote thread function
http://msdn.microsoft.com/en-us/library/windows/desktop/ms682437(v=vs.85).aspx

[13] Common Critera Part1
http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

[14] The Relationship between Information Asset Integrity and Availability for ICT Outsourcing. Nik Zulkarnaen Khidzir Azlinah Mohamed and Noor Habibah (paper)

Text Mining System For Non- Expert Miners

Ramya P
PG Scholar
SSN College of Engineering
Chennai, India

Sasirekha S
Assistant Professor
SSN College of Engineering
Chennai, India

***Abstract*--** Service oriented architecture integrated with text mining allows services to extract information in a well defined manner. In this paper, it is proposed to design a knowledge extracting system for the Ocean Information Data System. Deployed ARGO floating sensors of INCOIS (Indian National Council for Ocean Information Systems) organization reflects the characteristics of ocean. This is forwarded to the OIDS (Ocean Information Data System). For the data received from OIDS, pre-processing techniques are applied. Pre-processing involves the header retrieval and data separation. Header information is used to identify the region of sensor, whereas data is used in the analysis process of Ocean Information System. Analyzed data is segmented based on the region, by the header value. Mining technique and composition principle is applied on the segments for further analysis.

Index Terms-- Service oriented architecture; Text Mining; ARGO floating sensor; INCOIS; OIDS; Pre-processing.

I. INTRODUCTION

Text mining is described as the process of deriving high quality information from text. High quality information is derived from the patterns and trends. Text mining involves the processes of structuring the input text, deriving patterns from the structured data and finally the interpretation and evaluation of output.

View of text mining is an extension of data mining or knowledge from structured databases. Knowledge discovery from textual database refers generally to the process of extracting interesting or non-retrieval patterns or knowledge from unstructured text documents.

In today's competitive market, information is one of the main managerial assets since its analysis helps in effective steering. The concept of text mining is used in E-learning Web Miner Application [1]. It is a graphical user interface built with several operational modes for its users. For each mode of operation separate template was designed using Java.

Data mining technique in attrition analysis [2] is to identify a group of customers who have a high probability to attrite, and then the company can conduct marketing campaigns to change the behaviour in the desired direction. Nowadays the majority of large companies and corporations have to a greater or lesser extent a Data Warehouse and they use OLAP tools to extract and analyze the information which allows them to stand themselves in the market.

However, although there are areas where data mining techniques are being used more and more, such as business [3], marketing, education, banking, health and security systems, and so on , their use is still not generalized. This is mainly due to the fact that data mining projects need highly qualified professionals (expert data miners) to achieve, in reasonable time, useful results for business. One of the reasons for which expert data miners are required is that the knowledge discovery in databases (KDD) process involves multiple stages, and regretfully, in each one, there are a large number of decisions that have to be taken.

Data mining have induced interest [4] among the business community, particularly in large corporations with strong collection of data about their customers and business operations. Increased concentration towards business applications has necessitated even more requirements for knowledge discovery projects.

Extraction of information from the unstructured text [5], which will help all kinds of users. Information extraction typically is performed in the form of analysis pipelines. The pipeline stages are formant conversion, sentence splitting, tokenization, word stemming and annotation of tokens.

Mining technique in decision support system [6] is described with the temporal data. In this relationships between the events that affect the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

decision are discussed. This relationship is defined using the unsupervised learning technique of data mining. It not just defines the relationships between events, also extracts the interesting patterns and boundaries present in the system. The two methods of mining technique are supervised learning and unsupervised learning technique. Supervised learning technique is used in predictive statistical techniques whereas unsupervised learning method does not use dependent variables. It searches for the patterns and events.

This paper is organized in the following sections. Section 2 involves the system description and section 3 describes proposed work of the system. Section 4 gives the details of simulation results and finally Section 5 projects the conclusion.

II. SYSTEM DESCRIPTION

A system modelled to service all community is introduced in this paper. The concepts used to achieve this system are text mining and service oriented architecture. Services provided by the proposed system are fishing zone advisory and tsunami alerts. This can be performed by the analysis of ocean information. Ocean information is retrieved from the OIDS of INCOIS organisation. Data from the OIDS is pre-processed with some constraints as adding precision points to the processed data. Pre-processing is literally to minimize the difficulties in analysis process. Measurement of index value and pattern extraction becomes easier with the pre-processed data. From the measured values a graphical representation is obtained, which clearly states the system's performance.

III. PROPOSED WORK

Processing steps discussed in this paper are as follows: Pre-processing, Analysis, Exploration and Interpretation. Pre-processing step is generally defined as the data preparation process In this paper pre-processing step is for converting the hexa-decimal data to decimal data and adding precision values to the data.

Analysis process of this system involves the calculation of ocean index value. Index value is to represent the nature and mining technique is to extract interesting patterns of the system. Formula used to calculate the index value is,

$$N = 1.3247 - 2.5 \times 10^{-6}T^2 + S(2 \times 10^{-4} - 8 \times 10^{-7}T) + \frac{3300}{P^2} - \frac{3.2\times10^7}{P^4} \quad (1)$$

The parameters used in the index calculation are described as N is the oscillation index, T is the ocean temperature, S is the salinity of ocean water and P is the pressure value. Application of mining technique is known as the extraction process. As we are processing the ocean data, unsupervised learning data technique is applied in the here.

After the calculation of ocean index, association rule mining algorithm (an example of unsupervised learning method) is applied. It works by calculating the confidence and support metrics of the given data. Before this calculation, given data set is segmented by the time lag into events. The support of the rule is the number of times the rule holds same event in the database whereas confidence rate of an episode is calculated as,

$$r = \chi\,[\text{win a}] \Rightarrow \psi\,[\text{win c}] \quad (2)$$

The parameters win a, win c denotes the window values, ψ, χ are time delay values which are estimated as the time difference between the similar patterns. The interpretation technique is used to deploy the extracted results. Here composition technique is used as an interpretation. Composition is the principle of service orientation and is used to compose the results of different operating systems. The analysis results of the ocean data are composed using this principle. The composition process gives us the details of fishing zone and tsunami alerts respective to the areas. This result is documented in a table format with the necessary fields, denoting the analysis process.

IV. IMPLEMENTATION

A. Data Set

INCOIS is an acronym for Indian National Centre for Ocean Information System. It is an organization of central ministry department. This organization aims to provide a system which has the current analysis of ocean characteristics.

To achieve this it deploys ARGO floating sensors in the ocean, which reads the physical characteristics like temperature, salinity and pressure. The characteristic values are transmitted to OIDS (Ocean Information Data System) through satellites. Now the data received on OIDS is forwarded for the analysis process. In fig.1 the sample input dataset is given.

```
02602 2902102 65 32 K 2 2003-01-10 11:50:18.0 691 76.559 0.000 401647210
2003-01-10 12:49:18 1 EE 05
35 9D 89 3E 07 CB
37 09 89 54 07 62
38 30 89 63 06 FF
38 E7 89 67 06 A0
2014-05-01 00:46:47 1 9F 06 3A 40
89 68 06 3A
3B 5D 89 66
05 D5 3C 38
E1 C7 9E 3C
79 C3 8A 14
F0 B9 4A 12
F3 8E 39 F0
02602 321 34 73 32 K 2 2003-01-10 14:34:18 0.706 76.542 0.000 401647210
2003-01-10 14:28:18 1 4D 0B 70 B9
89 D2 00 E1
70 C9 89 D1
00 BE 70 D0
89 C9 00 A4
70 D7 89 C6
00 7C 70 E6
89 C4 00 6E
```

Fig.1 Dataset from OIDS

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

This dataset contains the sensor header value and data. Here data denotes the values of temperature, salinity and pressure. This data is pre-processed for the analysis process. Pre-process step involves the sensor header value extraction and data separation which is explained in Fig.2.

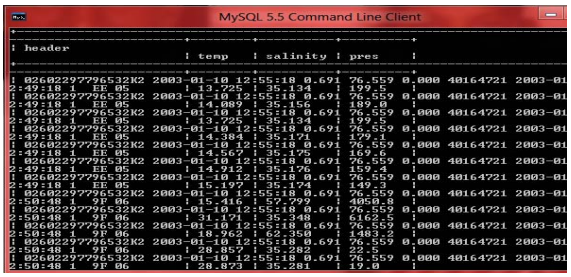


Fig.2 Separated Header and Data

Data is separated from the set and added with precision values in the pre-processing step. Also the header extracted from the set is used to distinguish the sensors deployed. After the separation data is segmented into regions using its header value. It is explained in Fig. 3.

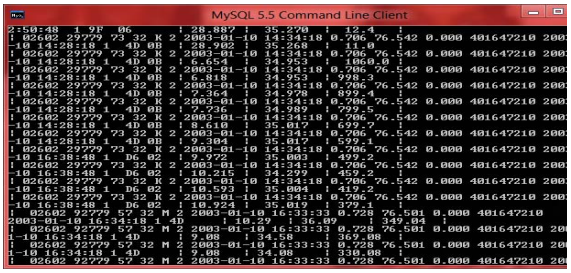


Fig.3 Region based segmentation

Data with same header values belong to a certain region are grouped in this step. Index value is estimated after the segmentation of regions and is given in Fig. 4.

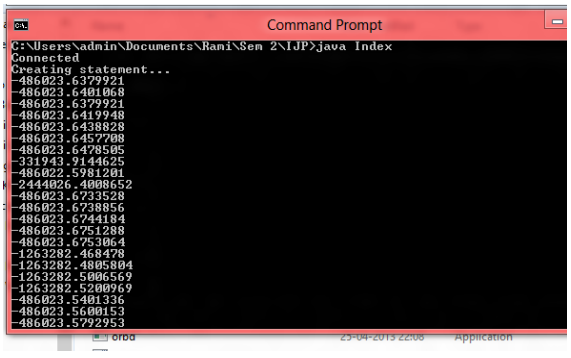


Fig .4 Ocean Index Value

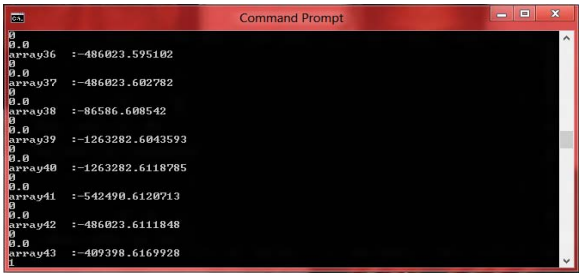


Fig.5 Support and Confidence metric

Fig.6 indicates the graphical representation of the time and index value. This plot has an average min and max values. When the index has its value lower or greater than its average min and max value, it is defined that the area might have strong waves.

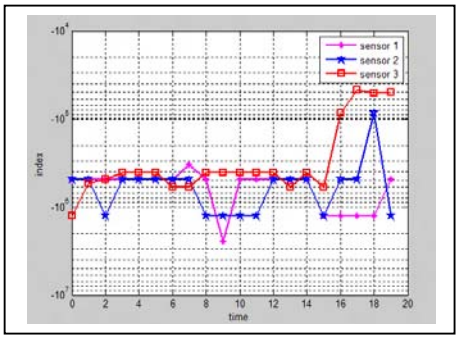


Fig.6 Analysis

Method to extract the similar pattern is depicted in fig.6. Here the value of confidence is plotted against the time value.

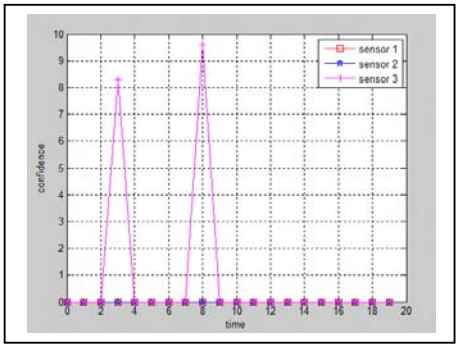


Fig.7 Time Vs Confidence

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

This graphical representation defines the fishing zone of the ocean. Inference obtained from the graph is that when the confidence value goes to its peak value with respect to time, then the area is referred as potential fishing zone.

V. CONCLUSION

Text Mining is a mining technique which extracts the characteristics of any system. In this project, it is proposed to generate a report about the ocean system. This report acts as a warning system of disasters like tsunami and storm. Also its information database contains the location of ores and mines under water, which increases the economy of our country. Tourism Board and Oil, Gas Producers of our country highly depending on the ocean for their growth. It helps the fisherman by listing the major fishing zones. It also used to alert the public at the time of disasters.

I. REFERENCES

[1] Marta Zorrilla, Diego García-Saiz (2012), "A service oriented architecture to Provide Data Mining services for Non-expert Miners," Decision Support Systems 55, Pages: 399–411, (2013).

[2] X. Hu, "A data mining approach for retailing bank customer attrition analysis," Applied Intelligence 22, Pages:47–60, (2005).

[3] H. Jiawei, K. Micheline, "Data mining: concepts and techniques," Elsevier Inc.,(2006).

[4] A. Arsanjani," Service-oriented modelling and architecture: How to identify, specify, and realize services," (2011).

[5] M.C. Chen, A.L. Chiu, H.H. Chang, "Mining changes in customer behaviour in retail Marketing," Expert Systems with Applications 28, Pages:773–781, (2005).

[6] S.Y. Kim, T.S. Jung, E.H. Suh, H.S. Hwang, "Customer segmentation and strategy development based on customer lifetime value: a case study," Expert Systems with Applications 31, Pages:101–107, (2006).

[7] Randy Kerber, Hal Beck, Tej Anand,Bill Smart, "Active Templates: Comprehensive Support for the Knowledge Discovery Process ",from KDD Processings.

[8] Seyed Mohammad Seyed Hosseini, Anahita Maleki, Mohammad Reza Gholamian, "Cluster analysis using data mining approach to develop CRM methodology to assess the customer loyalty," Expert Systems with Applications 37, Pages:5259–5264, (2010).

[9] Johannes Starlinger, Florian Lietner, Alfonso Valencia, Ulf Leser, "SOA based integration of Text Mining Services," Congress On Services-I, (2009).

[10] Q. Yang, X. Wu, 10 challenging problems in data mining research, "International Journal of Information Technology & Decision Making," Pages:597–604, , (2006).

[11] P.C. Wong, P. Whitney, J. Thomas, "Visualizing association rules for text mining, Proc. Of IEEE Symposium on Information Visualization," IEEE Computer Society, Pages:120–128, (1999).

[12] Sherri K. Harms, Jitender S.Deogun, "Sequential Association Rule Mining with Time Lags, Intelligent Information Systems 22:1, 7-22," (2004).

[13] R. Mazza, V. Dimitrova, "CourseVis: a graphical student monitoring tool for supporting instructors in web-based distance courses," International Journal of Human-Computer Studies 65 (2007) 125–139.

[14] E.W.T. Ngai, Yong Hu, Y.H. Wong, Yijun Chen, Xin Sun, "The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature," Decision Support System 50 (2011) 559–569.

[15] M.P. Papazoglou, W. van den Heuvel, "Service-oriented architectures: approaches, technologies and research issue," The VLDB Journal 16 (2007) 389–415.

[16] M.E. Zorrilla, E. Álvarez, "MATEP: monitoring and analysis tool for e-Learning plat--forms," Proc. 8th IEEE International Conference on Advanced Learning Technologies, Santander, 2008.

[17] T. Erl, "Service-Oriented Architecture: Concepts, Technology," and Design, 1st ed.Prentice Hall, 2005.

[18] A. Haira, D. Birant, A. Kut, "Improving quality assurance in education with web-based services by data mining and mobile technologies," Proc. of the 2008 Euro American Conference on Telematics and information Systems, ACM, New York, NY, 2009, pp. 1–7.

[19] U.M. Fayyad, G. Piatetsky-Shapiro, P. Smyth, R. Uthurusamy, "Advances in Knowledge Discovery and Data Mining Boston," AAAI/MIT Press, 1996.

[20] H. Jiawei, K. Micheline, "Data mining: concepts and techniques," Elsevier Inc., San Francisco, 2006.

[21] R. Hijon, A. Velázquez, "E-learning platforms analysis and development of students tracking functionality," in: E. Pearson, P. Bohman (Eds.), Proc. of World Conference on Educational Multimedia, Hypermedia and Telecommunications, Chesapeake, 2006, pp. 2823–2828.

[22] L. Feng, J. Yu, H. Lu, J. Han, "A template model for multidimensional inter-transactional association rules," The VLDB Journal 11 (2002) 153–175.

[23] D. Delen, "A comparative analysis of machine learning techniques for student retention management," Decision Support Systems 49 (2010) 498–506.

[24] I. Douglas, "Measuring participation in internet supported courses," in Proc. of the 2008 International Conference on Computer Science and Software Engineering, IEEE Computer Society, Washington, DC, 2008, pp. 714–717.

[25] Sudipto Guha, Rajeev Rastogi, and Kyuseok Shim, (1998), "ROCK: A Robust Clustering Algorithm for Categorical Attributes," In Proceedings of the 15th International Conference on Data Engineering, 1999.

[26] C.S. Potter, S. A. Klooster, and V. Brooks, "Inter-annual variability in terrestrial net primary production: Exploration of trends and controls on regional to global scales," Ecosystems, 2(1): 36-48 (1999).

[27] Pang-Ning Tan, Michael Steinbach, Vipin Kumar,Steven Klooster, Christopher Potter, Alicia Torregrosa, "Finding Spatio-Termporal Patterns in Earth Science Data: Goals, Issues and Results," Temporal Data Mining Workshop, KDD2001 (2001).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[28] G. H. Taylor, "Impacts of the El Niño/Southern Oscillation on the Pacific Northwest"(1998) http://www.ocs.orst.edu/reports/enso_pnw.html.

[29] M. Steinbach, P. N. Tan, V. Kumar, C. Potter, S.Klooster, A. Torregrosa, "Clustering Earth Science Data: Goals, Issues and Results", In Proc. of the Fourth KDD Workshop on Mining Scientific Datasets (2001).

[30] L. Ertöz, M. Steinbach, and V. Kumar, "Finding Topics in Collections of Documents: A Shared Nearest Neighbor Approach," Text Mine '01, Workshop on Text Mining, First SIAM International Conference on Data Mining, Chicago, IL, (2001).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

DNA Sequence Alignment using Hadoop in Cloud Computing Environment

Hamoud Alshammari
Department of Computer Science and Engineering
221 University Ave, University of Bridgeport,
Bridgeport, CT, USA

***Abstract*— Sequence Alignment process in DNA datasets faces different concerns, one of them is the complexity of finding any sequence since the data is unstructured and unrelated. Hadoop solves some of these issues by dividing the data into many blocks and manipulates these data perfectly with high efficient process. However, applying Hadoop has to be more accurate because DNA still needs more reliable and efficient solution because some problems might be not reliable via using Hadoop. In this project, I will explain until what extend Hadoop can solve the DNA sequence alignment with high degree of reliability.**

***Keywords*—** Cloud Computing, DNA Sequence Alignment, Hadoop, MapReduce.

I. INTRODUCTION

In bioinformatics, many applications need more time and a high degree of functional and computational capabilities either in hardware or software level to be applied. Hadoop and MapReduce solve this part of the capabilities by having a cluster and divide the data sets in the cluster, so not only the data is divided but the computation also is divided between the slaves in the cluster. In Hadoop we have the master node, which is the NameNode/JobTracker, and we have many slaves, which are DataNodes/TaskTrakers that store the data chunks/blocks and doing the computation themselves.

DNA chromosomes datasets can be considered as a big data even it is not very huge data but still unstructured and unrelated data. So, with this kind of data any process could have some complexities to be achieved with a high degree of reliability and efficiency. Hadoop divides the data into many blocks and store them on the DataNodes as a virtual file system, which is Hadoop Distributed File System HDFS. Different tools that support Hadoop to complete its job can be used to simplify the process of execution jobs as Zookeeper, Hive, Pig and so on [3].

Hadoop Distributed File System [Figure 1] allows the distribution of the data set into many DataNodes in the cluster that can be logically combed for processing. The process of distributing data in the cluster happens by selecting the size of the block in the Hadoop configurations. So, the user either stays with the default size, which is 64MB or changes it into 128MB [7]. Consequently, the job also is distributed into many tasks and each task gets executed on each TaskTracker on the local block/blocks.

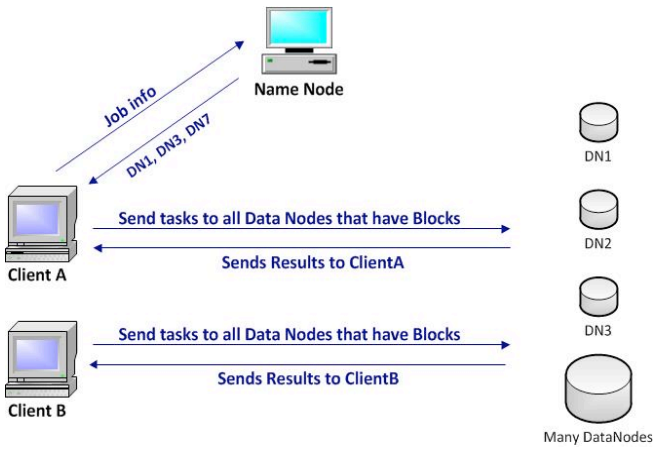


Figure 1: Hadoop MapReduce workflow.

In this project we will go through the issues that using Hadoop to manipulate the DNA data sets that cloud happened and we will propose a solution to skip these issues. In the second section, we will have a complete description of the DNA data format then in the followed section we will explain the problem and propose a solution to solve this problem. Then we will end up with some future work to have an efficient solution using Hadoop in DNA data sets.

II. DNA BACKGROUD AND DATA FORMAT

To have an efficient solution with any job on any data set, you have to understand the format of the data first and see if you can control it by having <key, value> on it or not. Understanding the data format is the important part of building a good MapReduce job. In this part I will explain the critical

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

areas in the DNA data sets that cloud cause a problem or weaknesses when execute some jobs on the blocks.

1) DNA background

DNA genome sequence consists of 24 chromosomes each consists of a huge size of sequence data (getting updated during the time) that is represented by an upper case English letters pairs. Each chromosome can be divided into many genes that are implemented by these pairs of letters. Scientists need to find some subsequences within these chromosomes to determine either some diseases or proteins frequently.

Each chromosome has many known genes and many unknown sequences. For example, chromosome one consists of about 249 million of nucleotide base pairs, which represent about %8 of the total DNA in human cells. The total number of genes in chromosome 1 is about 4,316 genes each one has different length of base pairs. There are about 890 known diseases that are related to this chromosome like Alzheimer type 4 [2][4]. From this briefly explanation about chromosome 1 you can imagine the data size of the DNA.

2) DNA data format

The most critical point here is the data format that from where the job reads the data. In DNA chromosomes, the data is unstructured and unrelated so the job needs to read the data carefully. [Figure 2] shows a part of the data that in the DNA and its structured [4]. As we can see, there is a line that has the metadata of the followed section, which is the sequence itself. So, based on the job type you can decide either you need to read some from this line or not. In sequence alignment example we need to read the name of the chromosome.

The other lines have the sequence of a part of that genome which is the letters (A, C, G, T and N somewhere). Writing a MapReduce job using some programming languages cloud be easy or difficult based on the job itself.

III. Proplem and Proposed Solution

1) Problem Definition

While the most of the sequences in the chromosomes are already defined, there are still frequent processes that reformulate and define these chromosomes with some updated data during the time. So, the process of finding any sequence still needed and the result could be different from the previous ones.

Having this type of unstructured data makes the process of finding a specific sequence very complicated and takes long time. So, with some online-processes the finding sequence process will cost the user some expenses with classical research techniques that he wouldn't have if he use the web-based distributed file system, which is supported by some models like Hadoop.

DNA data sets has a problem of Tow-line sequence which means the targeted sequence might be separated between two lines in the file. For example, if we have the targeted sequence is "GGGGCGATA" we might have it divided between two lines. This situation does not give an efficient solution because the divided sections will not be accounted in the solution.

The Two-lines sequence problem is shown in the sequences that are built in the NCBI project [5]. However, there might be another project in future could represent the data somehow but without having this problem.

```
>gi|157811750|ref|NW_001838574.2| Homo sapiens chromosome 1 genomic scaffold, alternate assembly HuRef SCAF_1103279180564, whole genome shotgun sequence
ATTACATTTTATTCCATTCCATTCCATTCCATTCCAGCACATTTCATTCCATTACATTCCTTTCGAGTCC
AATCCATTCCATTCCATTCCTATTGAGTCCATTCAATTCCATTCCATACCATTCGAGTCCATTCCATTCC
ACTCCATTCCATTCCATTCCATTCCATTCCATTCGCGTCCATTTCATTCCATTACATTACATTCCATTCG
AGTCCATTCCATACATTCCGTTAGACTCGAATCCATTCAATTCCATTCCATTCGCATACATTCCACTCCA
TTCCATTCGAGTCCATTCCATTCCATTCCATTCCACTCGAGTCCTTTCCATTCCATTCGAGTCCATTCCG
TTCTATTCCATTCCTTTCCAATCCATTCCTTTTCATACAGTCCATTCCAT
>gi|157811752|ref|NW_001838574.2| Homo sapiens chromosome 1 genomic scaffold, alternate assembly HuRef SCAF_1103279180564, whole genome shotgun sequence
TTATTCCATTCCATTCCATTCCATTCCAGCACATTTCATTCAGGACTTCCATTACATTCCTTTCGAGTCC
AATCCATTCCATTCCATTCCTATTGAGTCCATTCAATTCCATTCCATACCATTCGAGTCCATTCCATTCC
. . . . . .
. . . . . .
```


http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The main objectives behind this project are:

1. Speed up the process of finding a specific pattern by using Hadoop environment.
2. Build a MapReduce program to find a given sequence and how many this sequence is replicated in the specific chromosome or on all chromosomes.
3. Make the process of finding a specific pattern as speed as we can by executing this program in a cluster or by one machine.

2) Proposed Solution

To solve the two-lines sequence we need to test the length of the targeted sequence first and try to match whatever we have to find the results. In Hadoop, you can determine the format of the results e.g. yes/no result, number of matches either in whole DNA or in a specific chromosome. Generally, in Hadoop you can determine the format of the results based on the format of the data. Some data has line number on it, so you can determine the specific line that carries the result. Here is a part of the code that distributes data into lines then try to find match the sequence with the whole line to fine if they matched then add the counter by one.

```
String line = value.toString();
String sequence= "GGGGCGGGG";
Pattern pattern= Pattern.compile(s);

FileSplit filesplit= (FileSplit) context.getInputSplit();
Path path= filesplit.getPath();
String filename= path.getName();

String chrstring="";

for (String subline : line.split("\\W+"))
{
   if (subline.length() > 0) {
   chrstring = chrstring.concat(subline);}
}

Matcher matcher= pattern.matcher(chrstring);
int counter=0;
while (matcher.find()) counter++;

context.write(new Text(filename), new IntWritable(counter));
```

The above code solves the problem of finding the sequence in each line separately but we would solve the problem of Two-Lines sequence. So, we need to do some processes as follows:

1. Find the length of the sequence e.g. length is (SL).
2. Save the last digits of the sequence from the previous line with the length of (SL-1) and put that in a temporary string (Temp1).
3. Save the first digits from the current line with the length of (SL-1) and put that in a temporary string (Temp2).
4. Merge Temp1 with Temp2 to get a new line (Temp3= Temp1 + Temp2).
5. Now, we can apply the finding function on the new line (Tmep3).
6. We have to have this process between each two lines that could have Two-Lines sequence is separated between them.

There could be different solutions or additions to this solution to have it more efficient like testing (Temp1) if it matches the first digits of the sequence then go further with this solution. However, we need to do the testing process many times each has different length based on the previous length. Current length equals to the previous one minus one and so forth.

IV. Current Solution

In this proposed solution there is some overload work that cloud be solved by developing the solution to skips the non-beneficial data in DNA. There is a line in the beginning of each genome that carries the metadata of that genome, so we can skip reading this line but that will produce more work in the code to solve a tiny problem. So I preferred to leave it as it.

In addition, there is one more issue which the Unknown parts of the chromosome that have N on them. Also, we can consider that as a tiny overload work that we can skip or manipulate based on the job itself.

V. Future Work

As we mentioned previously, this project was applied on the data that we get from the NCBI project that formulated the data in files in the format that we explained in section II. So, I recommend the future work to solve the problem of Two-Lines sequence either by developing the current data files using one of the applications or by search and find another project that formulates the data with no Two-Lines sequence.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VI. CONCLUSION

Finding a sequence in DNA is very important process for many scientists fro many areas. However, we cloud have this process done by the regular searching ways but it will cost time and resources.

In this paper, we can see the weaknesses in the DNA chromosomes data from project NCBI that might cause a non-perfect job in the Hadoop Map/Reduce in the environment of Cloud Computing. So, by proposing a solution above, we could solve the Two-Lines sequence data. In the future work section, we described some of points that might help to have more efficiency and functionality.

REFERENCES

[1] A. McKenna, M. Hanna, E. Banks, A. Sivachenko, K. Cibulskis, A. Kernytsky, K. Garimella, D. Altshuler, S. Gabriel, and M. Daly, "The Genome Analysis Toolkit: a MapReduce framework for analyzing next-generation DNA sequencing data," Genome research, vol. 20, pp. 1297-1303.

[2] H. Mathkour and M. Ahmad, "Genome Sequence Analysis: A Survey," Journal of Computer Science, vol. 5, 2009.

[3] Hadoop, "Hadoop: http://hadoop.apache.org/, accessed on 15 May 2014," 2014.

[4] National Center for Biotechnology Information project, "ncbi.nlm.nih.gov/genome/guide/human/, accecced on 15 May 2014", 2014.

[5] Rout, S. B., Mishra, B. S. P., & Dehury, S. (2013, February). Hadoop Cloud Application In DNA Alignment And Comparison. In International Journal of Engineering Research and Technology (Vol. 2, No. 7 (July-2013)). ESRSA Publications.

[6] Schatz, M. C., Langmead, B., & Salzberg, S. L. (2010). Cloud computing and the DNA data race. Nature biotechnology, 28(7), 691.

[7] Shvachko, K.; Hairong Kuang; Radia, S.; Chansler, R., "The Hadoop Distributed File System," Mass Storage Systems and Technologies (MSST), 2010 IEEE 26th Symposium on , vol., no., pp.1,10, 3-7 May 2010.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VIDEO GAME USER INTERFACE DEVELOPMENT USING SCALEFORM Gfx (CLIK™ AND SCALEFORM 3Di™)

Oluwafemi J. Ayangbekun[#1], Ibrahim O. Akinde[*2],

[#]*Department of Information Systems, Faculty of Commerce,*
University of Cape Town, South Africa.
[1] phemmyc@yahoo.com

[*] *Department of Computer Science, Faculty of Information and Communication Technology,*
Crescent University, Abeokuta, Nigeria.
[2] ibmaxx@hotmail.com

***Abstract* — This paper explains how Scaleform Gfx technology can be used to create a beautifully rendered Front-End Menu using Flash Professional's proprietary language, ActionScript, both in 2D and 3D for video game development. Scaleform Gfx is cutting edge technology designed by Autodesk for creating stunning user interfaces.**

This paper introduces Scaleform Gfx as videogame middleware, reviews some of the previous games' user interfaces designed with Scaleform Gfx, provides an iteration of steps that can serve as a framework for creating a fully functional front-end menu and discusses the limitations of Scaleform Gfx.

Also, this paper introduces Scaleform CLIK and Scaleform 3Di and explains how interoperable they are with each other when developing a user interface.

I. INTRODUCTION

Video game development is usually a very tasking process because of all the numerous development highlights like programming, level design, lighting, rendering, concept design and so much more. But more than half of the entire development effort usually goes to developing the user interface. The user interface may be the Front-End Menu, the Heads-Up-Display or even an Inventory Menu. What makes the user interface so important? The answer is simple. Without the user interface, there is no interaction between the user and the game. A user interface is simply the system by which people (users) interact with a machine. A video game's user interface is the conduit between the player and the game. It is all that stands between the user and the game. But developing the user interface is not nearly enough. Aesthetics can help to improve the overall audio and visual appeal of the interface to be used, hence simulating the effect of "gluing the user to the screen". That is where Scaleform Gfx comes in.

Autodesk® Scaleform Gfx® enables developers to leverage the power of the Adobe® Flash® tool set to create powerful and immersive user interfaces. Scaleform Gfx provides a streamlined solution to create hardware-accelerated 3D game menus, HUDs, animated textures, in-game videos, and mini-games and is used in over 1,000 AAA titles across all major platforms. It is integrated with some game engines like Unreal Engine 3 and 4 and can be installed as a plugin for others like Unity 4 and CryEngine 3. As opposed to the batch computing era and command-line era where the entire user interface was in black and white (MS-DOS), and as opposed to other software with user interface development capabilities as a side attraction, Scaleform Gfx can be used to create very complex, powerful, immersive and detailed interfaces that run at smooth 60fps.

User interfaces usually include the hardware (physical) and software (logical) components. Whether or not the designer(s) focuses on either or both of the logical or physical components, user interfaces must provide a means of:

- Input, allowing the users to manipulate the system
- Output, allowing the system to indicate the effects of the users' manipulation

Hence, the major goal of user interface design and development is to improve the interactions between the users and computers by making computers more usable and receptive to the users' needs. The added boon of Scaleform Gfx is that user interfaces developed with Scaleform Gfx can do all that while also rendering aesthetically pleasing and extremely powerful views.

II. WHAT IS SCALEFORM GFX?

Scaleform Gfx is the leading Flash-based user interface (UI) middleware for the video-game industry. Scaleform Gfx combines the performance of hardware accelerated 3D graphics technology with the proven productivity and workflow of Adobe Flash tools to help developers rapidly create highly immersive 3D UI and casual game experiences [8]. Its key features are:

- It provides for anti-aliased vector graphics which allow developers to create fully-fledged menus with

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

scrollbars, option steppers, HUDs, and checkboxes and so on [2].
- It provides a high-quality dynamic font system which renders fonts into vector images which can be used to render text fields with low memory cost [2].
- It supports rich text support including different colours, smileys, and fonts – basically anything that can be included in a text field [2].
- It supports masking for arbitrary shape clipping and shape animation. This is important for animations of shapes that are not regular like rectangles. An example is a heart-shaped animation [2].
- For artists and designers, especially those that use Photoshop and other Image-editing software, Scaleform Gfx allows for changing in blend modes and filter effects like 'Glow', 'Multiply', and 'Drop Shadow' and these can be applied to both text and images [2].
- While Scaleform Gfx is primarily a 2D tool, Scaleform Gfx provides extensions for Flash 10 and up that allow for 3D translations and transformations like tilting on the axes and moving from point A to B. These extensions make up Scaleform 3Di [2].
- Scale9Grid enables developers to resize user interfaces easily and solves the problem of cross-platform development [2].
- Scaleform Gfx 4 features a multi-threaded back-end design and is integrated with the Unreal Engine 4 which is also a multi-threaded game engine [7]. Multi-threading is the concept of breaking a program into two or more parts called threads which run in parallel to improve effectiveness, responsiveness and performance.

A. Scaleform CLIK

The Scaleform Common Lightweight Interface Kit (CLIK) allows developers to rapidly prototype efficient front-end menu interfaces for games, and then take those prototypes to completion by skinning [2]. Skinning is the process of applying, adding or replacing the base components of the interface with more detailed, production ready components without necessarily changing the workflow of the interface. The kit contains buttons, checkboxes, scrollbars, radio buttons, option steppers and every other component that can be used to design a user interface.

B. Scaleform 3Di

Scaleform 3Di uses hardware accelerated triangles to render shapes. What this means is that it uses the capabilities of the graphics card to render objects in 3D. Scaleform 3Di contains extensions to enable the manipulation of 2D objects in 3D space. When an object has both 2D and 3D properties, the 3D properties are applied before the 2D properties. This detail is important to understand to get the expected results when rotating an object or translating it [1].

The 3Di extensions are:
- ._xrotation: This increases or decreases the rotation of an object on the x-axis.
- ._yrotation: This increases or decreases the rotation of an object on the y-axis.
- ._perspfov: This extension controls the perspective distortion of a 3D object. The lower the value, the less the distortion. By default, its value is 55 degrees but it can be assigned any value between 1 and 179 degrees.
- _z: This translates an object along the z-axis. The lower the value, the closer the object translates to the screen.
- _zscale: This alters the scale of any z-axis translation. It functions identically to _xscale and _yscale. It defaults to 100 or 1:1 ratio.
- _matrix3d: This allows developers to set the complete 3D transform of an object using an array of 16 floating point numbers, making it a 4 x 4 matrix. Whenever any of the previously mentioned extensions are used on an object, Scaleform Gfx will automatically apply a 3D matrix to that object and bring it into 3D space. After that, the only way to return that object to 2D is to set that matrix to null. It is available as a low-level option for programmers who want to create some unique transformations.

Scaleform 3Di does have a few limitations:
- There is no depth-sorting. This means that when objects are rotated or translated, they may not be in the right order over or under other objects as expected. This is because the draw order is determined by the layer order in Flash, not their positions in 3D space [8].
- There is no back-face culling. This means when an object is rotated, the back side will be drawn. Unless this is the effect desired, rotation should be limited to 90 degrees in either direction [8].

III. USER INTERFACES DEVELOPED WITH SCALEFORM GFX

Here is brief list of gaming titles that have used Scaleform Gfx in recent years:
Starforce Battlement, Batman: Arkham Origins, Killer is Dead, Lost Planet 2, Dragon Age 2, Crysis 2, The Witcher 2: Assassins of Kings, Borderlands 2, DC Universe Online, Street Fighter IV, Dragon Age Origins, Mass Effect, Mass Effect 2, Prototype, Fable II, Fable II: Pub Games, Civilization Revolution, Civilization IV, Civilization IV: Beyond the Sword, , Civilization IV: Warlords, , Civilization IV: Colonization, Halo Wars, 007: Quantum of Solace,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Railroads!, Kung Fu Panda, Viva Pinata: Party Animals, Mafia II, SFVT Shots, and Trivium, to name but a few. We take a look at a few examples of user interfaces mentioned above that are very crucial to this research.

A. Starforce Battlement

Starforce Battlement is a tower defence game with role-playing game elements. The primary objective of each level is to prevent oncoming waves of enemies from reaching their destination. Every enemy that reaches the destination subtracts one point from the player's life. If enough enemies reach the destination, the player's life is reduced to zero and the game is over. Starforce Battlement is written entirely in ActionScript 3 and leverages Scaleform Gfx's 'Shippable Mobile Player' for cross-platform deployment. It goes without saying that the whole game is like a giant cluster of user interfaces. The Main Menu allows the player to select a mission and provides additional options for changing the player's technology tree and viewing tutorials, the player's statistical history, and the player's achievements. The buttons at the top left of the Main Menu allow the player to toggle music, toggle sound effects, or exit the game. Level selection consists of indicators placed on the galaxy/nebula map which the player can select. Each nebula contains a set of missions that are unlocked in a linear progression. The player can drag the map around in 2D space to explore available options before selecting a particular mission. When the player selects an available mission, the Mission Data View (MissionDataView.as) is displayed. The Mission Data View provides the player with details about the mission. From this view, the player may either launch the mission by selecting the "Enter Mission" button or may return to the Mission Select View by selecting the "X" button at the top right of the view.

B. Batman: Arkham Origins

Developed in 2013, Batman: Arkham Origins is an action-adventure video game published by Warner Bros. Studios. The user interface features a very sleek menu design as soon as the player gets into the game and past the splash screens. The Menu features buttons that change their states depending on whether the player's cursor is clicking on them, hovering over them or not hovering over them at all. In the background there is a rather obvious cascade of slides that blur the line between image and video. The game's user interface accepts input from both a combination of the keyboard and mouse and from gamepads.

C. SFVT Shots (Street Fighter versus Tekken™)

SFVT Shots is mobile app that displays high resolution screen grabs of the popular game Street Fighter Versus Tekken. The images displayed can be rotated and tilted on every axis (Figure 1). Swipes on the screen allow for the interface to display the next or previous image as intended by the user and each iteration in the image swiping process presents the new image with a different transition. The next update for the game will allow images to be dynamically saved to the app. The app will be available for free soon on the Google Play store.

Fig. 1: SFVT Shots.

D. Trivium

Trivium is a new mobile game still under development (our main video game design for this research) for Android. The menu prototype was created entirely with Scaleform CLIK and 3Di but it has not been skinned yet. Trivium is a trivia game for anime fans all over the world and features a dynamic score system, a dynamic timer system, an achievement system and an Inference Engine. Upon completion, the game will be available for purchase on the Google Play store.

IV. CREATING A SIMPLE FRONT-END MENU WITH SCALEFORM GFX

This section will detail the steps necessary to create a front-end game menu for a video game called Trivium. Trivium is an indie flash trivia game targeted at anime (Japanese-themed cartoon) audiences all over the world. As with Starforce Battlement, Trivium is written entirely in ActionScript and utilizes both Scaleform CLIK and Scaleform 3Di. Note that all the steps taken here are implemented in Flash Professional (Fig. 2).

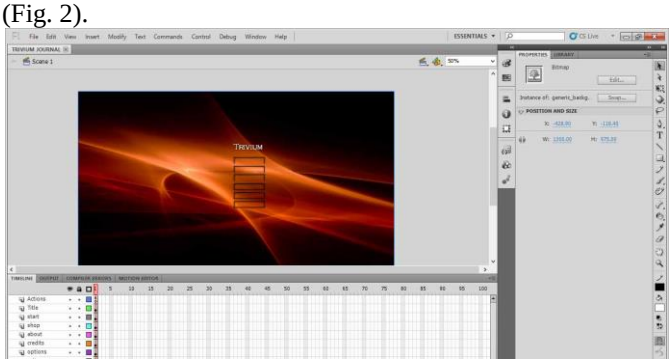


Fig. 2: Trivium in Flash Professional

The custom user interface that will be created in this document will have the following workflow:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

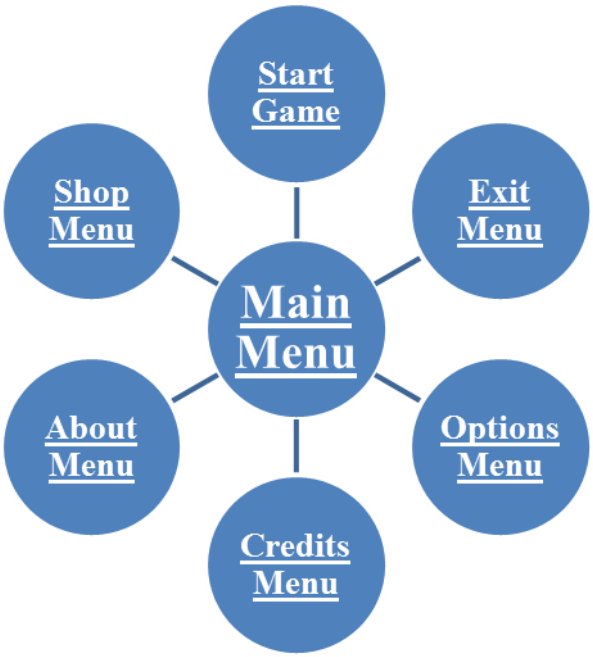


Fig. 3: Front-End Menu Work Flow.

After configuring CLIK and installing the Scaleform Launcher in Flash [6], development commences immediately in the following steps:

- Draw a sketch of what the Front-End Menu looks like (Concept Design – Fig. 3).
- Design all art assets to be used in Photoshop or any other Image Editing Software.
- Open the CLIK AS2 file and copy the library.
- Open a new file in Flash. Set the language to ActionScript 2. Save the file as Front-End Menu_Prototype.fla.
- Paste in the library of CLIK AS2 into Menu_Prototype.
- Import all art assets into Front-End Menu_Prototype.fla.
- Create a new layer called 'Background'. Drag and drop the background asset(s) to the scene while remaining on the layer according to the concept design.
- Create a new layer called 'Main Menu'. Click on the 'Shapes' tool. Draw a rectangle whose width and height are more than the scene's width and height. Change its fill property to empty.
- Save the rectangle as 'Rec' of type movieclip by dragging it into the library.
- Delete the rectangle on the scene. Drag and drop an instance of Rec onto Frame 1 of Man Menu. In the instance name field, type in 'menu_container'.
- Create another layer called 'Actions'. All other layers except 'Labels' should be below this layer.
- Double-click on menu-container. Create 7 new layers and name them 'Actions 2', 'Startbtn', 'Shopbtn', 'Aboutbtn', 'Creditsbtn', 'Optionsbtn' and 'Exitbtn'. The last layer called 'Layer 1' is where the rectangle resides. Rename it as 'Rectangle'.
- Drag and drop one Button to each of the layers except Rectangle. No work is going to be done on Rectangle. It simply acts as the visualization of the placeholder of the menu. In the instance name field, type in 'startbtn', 'shopbtn', 'aboutbtn', 'creditsbtn', 'optionsbtn' and 'exitbtn'.
- Create 7 new layers. Name them 'Start Menu', 'Shop Menu', 'About Menu', 'Credits Menu', 'Options Menu', 'Exit Menu'. Go to Frame 2 of Start Menu. Insert a button with instance name 'backbtn. Insert backbtn on Frame 3 of Shop Menu, Frame 4 of About Menu, Frame 5 of Credits Menu, Frame 6 of Options Menu and Frame 7 of Exit Menu.
- To use Scaleform 3Di to apply transformations and translations to our buttons, click on Frame 1 of Actions 2 and type in:

```
//To translate each button along the z-axis so each one appears offset to another
        startbtn._z=-50;
        shopbtn._z=130;
        aboutbtn._z=79;
        creditsbtn._z=32;
        optionsbtn._z=150;
        exitbtn._z=100;
//To change the cursor button to the hand button when the cursor is on the buttons and to enable mouse clicks on the buttons
        startbtn.buttonMode= true;
        shopbtn.buttonMode=true;
        aboutbtn.buttonMode=true;
        creditsbtn.buttonMode=true;
        optionsbtn.btnMode=true;
        exitbtn.btnMode=true;
```

- Do the same for all the buttons called 'backbtn'.
- To go to the respective sub menus when each button is clicked on:

```
        startbtn.addEventListener(MouseEvent.CLICK, startmenu);
        function startmenu(event:MouseEvent):void
        {
```


http://sites.google.com/site/ijcsis/
ISSN 1947-5500

```
gotoAndStop(2); }
shopbtn.addEventListener(MouseEvent.CLI
CK, shopmenu);
function shopmenu(event:MouseEvent):void
{
gotoAndStop(3); }
aboutbtn.addEventListener(MouseEvent.CL
ICK, aboutmenu);
function
aboutmenu(event:MouseEvent):void {
gotoAndStop(4); }
creditsbtn.addEventListener(MouseEvent.C
LICK, creditsmenu);
function exitmenu(event:MouseEvent):void
{
gotoAndStop(5); }
optionsbtn.addEventListener(MouseEvent.C
LICK,optionsmenu);
function
optionsmenu(event:MouseEvent):void {
gotoAndStop(6); }
exitbtn.addEventListener(MouseEvent.CLI
CK, exitmenu);
function
exitmenu(event:MouseEvent):void{
gotoAndStop(7); }
```

- To go back to the Main Menu when any 'backbtn' is clicked on, type this on each frame of the Actions layer where backbtn resides:

```
backbtn.addEventListener(MouseEvent.CLI
CK, gobacktomainmenu);
function
gobacktomainmenu(event:MouseEvent):void {
gotoAndStop(1); }
```

- Go back to the original scene and click on Actions. Type in:

```
//Create four variables xvar, yvar, xhold, yhold that
hold four different values.
/* Functions rotatex and rotatey rotate the movieclip
menu_container. Both functions are called every
frame by the function 'beginidlerotateloop'*/
var xvar:Number=0.030
var yvar:Number=0.035
var xhold:Number=10;
var hold:Number=15;
function rotatex(mc:MovieClip):void
{
/*set menu_container's rotation on the x-
axisto be equal to its rotation plus xvar
every frame */
mc._xrotation= mc._xrotation +
xvar;
/*if menu_container's rotation value is
greater than xhold or less than negative
xhold, change xvar to negative xvar, thereby
rotating in the opposite direction */
if (mc._xrotation>xhold ||
mc._xrotation< -xhold)
{
xvar= -xvar
}
}
function rotatey(mc:MovieClip):void
{
/*set menu_container's rotation on the y-
axisto be equal to its rotation plus yvar
every frame */
mc._yrotation= mc._yrotation +
yvar;
/*if menu_container's rotation value is
greater than yhold or less than negative
yhold, change yvar to negative yvar, thereby
rotating in the opposite direction */
if (mc._yrotation>yhold ||
mc._yrotation< -yhold)
{
yvar= -yvar
}
}
//Call functions rotatex and rotatey every
frame
function beginidlerotateloop():void {
onEnterFrame = function() {
rotatex(menu_container);
rotatey(menu_container);
}
}
```

- To change the Main Menu's field of view as it rotates, type in:

```
//change menu_container's field of view to
70 degrees
menu_container._perspfov=70;
```

Figure 4: Trivium using Scaleform Gfx.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

In the 20 steps iterated above, Scaleform 3Di and Scaleform CLIK were used to create a front-end menu prototype that tilts back and forth on both the x-axis and y-axis with fully functioning clickable buttons that can go to each individual sub-menu and go back to the main menu when the back button is pressed.
This simple framework can be used to design user interfaces that are so complex with so many nested movieclips, while running smoothly at 60fps.

V. CONCLUSION

This paper presented one possible way to use Scaleform CLIK and Scaleform 3Di. There are many permutations, and most projects will present unique challenges. The framework given above in the form of steps enables developers to design and develop fully fledged user interfaces, particularly the Front-End Menu. However, it can also be used for developing Heads-Up-Displays as only a few changes need be made. For example, the button system might be removed altogether and replaced with screens, boxes and bars to display the user's health points, status, or location on the map. The common denominator, however, is that Scaleform Gfx is a really powerful tool that can be used to create really complex user interfaces in minutes, not days and should be utilized by every user interface designer in the video game industry.

VI. RECCOMENDATIONS

As great as Scaleform Gfx is, it could still be improved. Scaleform 4 would be expected to support multi-threading as mentioned in Section 2.1 and also be integrated into game engines like Unreal Engine 3, CryEngine 3 and Unity 4, instead of having to download plugins. Also, depth-sorting and back-face culling problems limit the options of imaginative developers and should be remedied.
Finally, as mentioned above, Scalefrom Gfx is recommended for any user interface designer in the market as it is indeed the leading Flash-based user interface development middleware today.

REFERENCES

[1] Autodesk (2010): "Intro to Scaleform for UI". Scaleform Gfx Video Tutorial. USA.

[2] Autodesk (2010): "3Di Overview". Scaleform Gfx SDK Documentation. Page 1 – 40. USA.

[3] Autodesk (2010): "Autodesk & Scaleform Gfx". Scaleform Gfx SDK Documentation Page 1- 30.. USA.\

[4] Autodesk (2010): "Mobile Game Kit Overview". Scaleform Gfx SDK Documentation. Page 1 – 35. USA.

[5] Autodesk (2014): "Scaleform Gfx CLIK User Guide AS3". Scaleform Gfx SDK Documentation. Page 1 – 40. USA.

[6] Autodesk (2014):"sf_4.2_getting_started_with_CLIK". Scaleform Gfx SDK Documentation. Page 1 – 41. USA

[7] Kris Graft (2010): "Scaleform Gfx GFx 4 Supports Flash 10 AS3". Gamasutra. Page 1. USA.

[8] Mathew Doyle (2010): "Using 3Di Flash AS2 Extensions". Scaleform Gfx Video Tutorial. USA.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Bovines Muzzle Identification Using Box-Counting

Hazem M. El-Bakry
Department of Information Systems,
Faculty of Computer and Information Sciences,
Mansoura University, Mansoura, Egypt

Ibrahim El-Hennawy
Faculty of Computer Science and Information ,
Beni-Suef University
Beni-Suef, Egypt

Hagar M. El Hadad
Faculty of Computer Science and Information,
Beni-Suef University
Beni-Suef, Egypt

Abstract— **Bovines identification has become widely used as essential for guarantee the safety of cattle products and assists veterinary disease supervision and control. Texture feature extraction is a key step for muzzle image processing. In this paper, we focus on bovines muzzle patterns identification as a biological texture using a method for feature extraction of Muzzle images. The proposed method has been implemented by using Box-counting Fractal Dimension. Before texture feature extraction, preprocessing operations such as histogram equalization and morphological filtering (opening and closing) have been used for increasing the contrast and remove noise of the image. After that, fractal dimension is calculated as the texture feature. The experimental results show that feature vector for different image of the same muzzle are highly symmetry. Therefore, it can be applied in registration of bovines for breeding and marketing systems.**

Keywords-component; bovine's identification, image processing, fractal dimension, feature extraction, Box-counting

I. INTRODUCTION

Nowadays Veterinarians do great effort in the livestock field. Bovines identification is used for exhibition of bovines, breeding and marketing. Early bovines identification method such as ink printing method has disadvantage that is the good muzzle print take time reach up to 6 minutes [1] and the difficulty in obtaining. Also ink print method problems are not holding the animal still, the use of too much ink, a build-up of moisture on the animal's nose and result in unreadable print [2].

In humans we use fingerprint as biometric identifier and in bovines hair covered animal skin except some parts such as muzzle. The distribution of ridges and valleys in each cattle muzzle is responsible for forming bovine's pattern. Because of the muzzle consistent over time so it use as like fingerprints of human to form biometric identifier. Bovines pattern is hereditable and asymmetry between each half is meaningful [3]. Now we captured a life image of cattle and do some image enhancing and feature extraction methods to automatically identify muzzle patters than ink printing method then we use mathematical morphology filtering in order to use it in bovine's identification [4].

Lot of improves has been done of texture feature extraction than past 50 years. Texture feature extraction is a key fundamental in image classification and segmentation [5]. First applying histogram equalization on image that produce a gray scale which makes all pixels values closed as possible to contrast adjustment and enhancement. Then by using Mathematical morphology filtering noise in the image can be removed effectively. So after histogram equalization the low contrast image transformed into high contrast images and noise removed after applying opening and closing operations on the image.

The fractal dimension is calculated as the texture feature of image. The fractal dimension of an image can reflect the image feature, so some measures are taken to have the direction details of the image to better express the important texture feature information in Muzzle image.

The rest of the paper is organized as follows. Image Pre-processing used in this paper is described in Section II. Feature Extraction is detailed introduced in Section III. In Section IV Experimental result is presented. Conclusion AND Future Work are reported in section V.

II. IMAGE PRE-PROCESSING

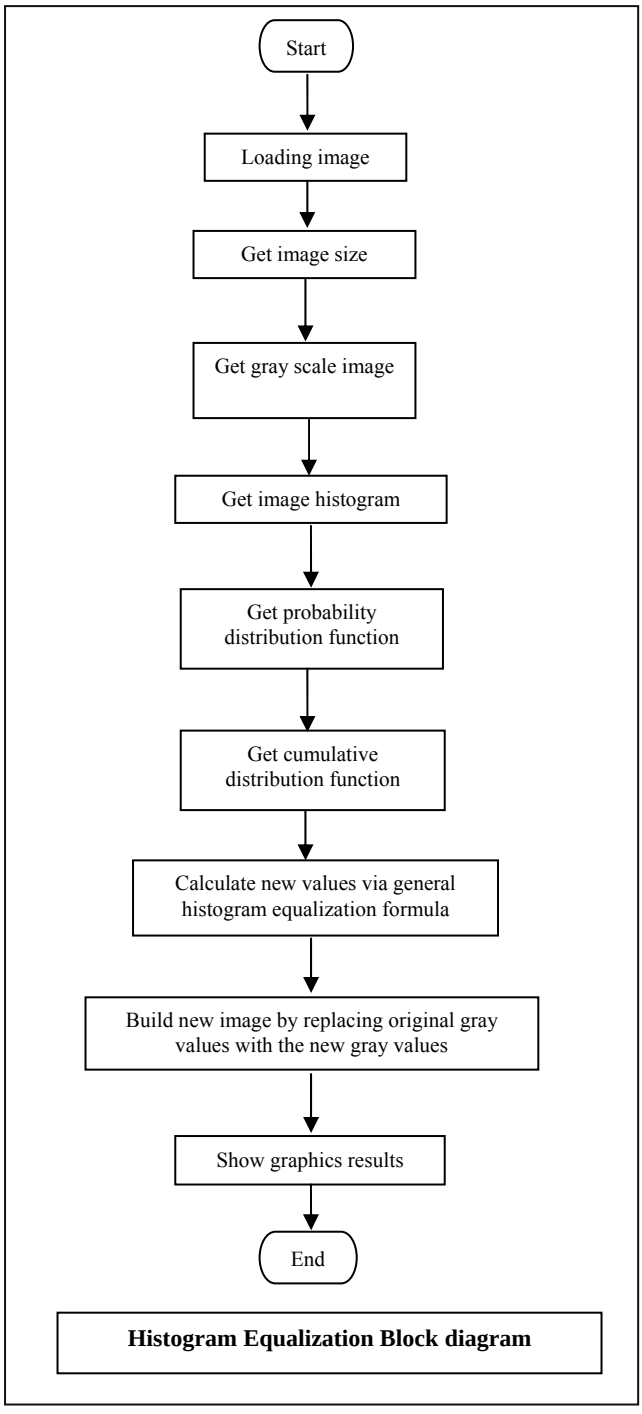
Image pre-processing is applied at the lowest level of elimination and its aim is to reduce undesired noises and enhance the image data which is important for further processing [6]. It is required for improving the performance of image processing methods such as image segmentation and image feature extraction [7][8]. Image pre-processing operations such as histogram equalization (HEQ) to increase the contrast of each image and mathematical morphology filtering (MM) to remove image noise must do before texture feature extraction [23-46].

A. Histogram equalization (HEQ)

First, histogram is the probability distribution of a particular type of data. One type of histogram is image histogram which gives us graphical representation of the distribution of the gray values in a digital image. Image's histogram analyzes the frequency of appearance of the different gray levels contained in the image. Histogram equalization spreads out intensity values along the total range of values in order to achieve higher contrast. This algorithm is useful in image which is represented by close contrast values, such as images in which both the background and foreground are bright at the same time, or else both are dark at the same time [9].

Histogram equalization method is implemented as shown in the following flow chart that outlining the following steps.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500



Histogram Equalization Block diagram

- Consider a digital image with gray levels in the range [0, L−1], Probability Distribution Function of the image can be computed as equation (1):

$$P(r_k) = \frac{n_k}{N} \qquad k = 0, \ldots, L-1 \qquad (1)$$

Where r_k is the k_{th} gray level and n_k is the number of pixels in the image having gray level r_k .

- Cumulative Distribution Function (CDF) can also be computed as followed:

$$C(r_k) = \sum_{i=0}^{k} P(r_i) \qquad (2)$$

K = 0,.....L -1 , $0 \leq C(r_k) \leq 1$

- Histogram Equalization (HE) appropriates gray level S_k to gray level r_k of the input image using equation (2). So we have:

$$S_k = (L-1) \times C(r_k) \qquad (3)$$

- Gray level S_k 's changes can be computed in usual histogram equalization method:

$$\Delta S_k = (L-1) \times P(r_k) \qquad (4)$$

Equation (4) means that distance between S_K and S_k +1 has direct relation with PDF of the input image at gray level r_k [10].

B. MATHEMATICAL MORPHOLOGY FILTERING (MM)

Morphology means the study of shape. Mathematical morphology describes shapes by using set theory, lattice theory, topology, and random functions depending on mathematical theory. In image processing, mathematical morphology used to determine the interaction between image by using some operations such as erosion, dilation, closing and opening. Here in this paper first we do opening operation on the image followed by do closing operation on the image in order to remove noise points, fill the edge of some pixels, remove small lines and connect thin break areas in muzzle image [11].

- Dilation and erosion operations are not inverse operators. If X is eroded by B and then dilated by B, one may end up with a smaller set than the original set X. This set, denoted by X ○ B, is called the opening of X by B defined by X ○ B = $(X \ominus B) \oplus B$. Likewise the closing of X by B is the dilation of X followed by the erosion, both with the same structuring element. The closing of X by B may return a set which is larger than X; it is denoted by X ● B and defined by X ● B = (X $\oplus$ B) $\ominus$ B.

- Dilations and erosions are closely related. This is expressed in the principle of duality [12] that states that

$X \ominus B = (X^c \oplus \check{B})^c$ or $X \oplus B = (X^c \ominus \check{B})^c$.

Where the *complement* of X, denoted X^c, is defined as $X^c = \{x \mid x \notin X\}$, and the *symmetric* or *transposed* set of B $\subseteq E$ is the set defined as $\check{B} = \{-b \mid b \in B\}$. Therefore all statements concerning erosions and openings have a parallel statement for dilations and closings, and vice versa [13].

- The opening of *A* by *B* is obtained by the erosion of *A* by *B*, followed by dilation of the resulting image by *B:*

$$A \circ B = (A \ominus B) \oplus B$$

- The closing of *A* by *B* is obtained by the dilation of *A* by *B*, followed by erosion of the resulting structure by *B*:

$$A \bullet B = (A \oplus B) \ominus B$$

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

III. FEATURE EXTRACTION

Image feature extraction is very important in many image processing applications such as classification and recognition. In this paper we use box counting algorithm feature extraction methods. This algorithm is implemented for texture analysis of muzzle database.

A. *Texture feature extraction using box counting method:-*

Texture feature extraction is the second step after preprocessing operations. Some transforms performed in the resulting image (closed image). There are found several methods to calculate fractal dimension of muzzle image, but a lot of studies show that box counting algorithm is common used in fractal dimensions calculations [14]. Gang pain and Roques-Carm advanced this method [15]. Sarker and chaudhuri upgrade this algorithm to differential box counting [16][17][18][19].

Fractal appears in image application such as analysis, segmentation, classification pattern recognitions etc. [20]. Fractal dimension (FD) is valuable feature in texture segmentation and muzzle image classification. Box counting technique frequently used to estimate fractal dimension of muzzle images. The box counting algorithm is useful for determining fractal properties of 1D segment, a 2D muzzle image or a 3D array. Box counting method is the most frequently used and more popular algorithm. Here the box counting algorithm steps. The box counting dimension associated with the concept of self-similarity where a muzzle image sub-divided into smaller elements and each small part replace the original muzzle image. Box counting dimension algorithm Db of any bounded subset of A in R n, which is a set in Euclidean space. Let Nr(A) be the smallest number of the set of r that cover A. Then

$$D_b(A) = \quad (5)$$

Provided that the limit exists.

Subdividing R^n into a lattice of grid size r×r where r is continually reduced, it follows that $N'_r(A)$ is the number of grid elements that intersect A and D_b is,

$$D_b(A) = \quad (6)$$

Provided that the limit exists. This implies that the box counting dimension *Db and Nr(A) are related by the following power law relation,*

$$(7)$$

Proof of this relation can be obtained by taking logs of both sides of equation (7) and rearranging to form equation (8),

$$\log N_r(A) = \quad (8)$$

From equation (8) it is possible to make an analogy to the equation of a straight line, y = mx ± c, where m is the slope of the line and c is the y intersect. The box-counting dimension is implemented by placing a bounded set A, in the form of a muzzle image, on to a grid formed from boxes of size r ×r . Grid boxes containing some of the structure, which in the case of a muzzle image is represented by the grey-levels within a certain range, are next counted. The total number of boxes in the grid that contain some of the structure is N (A) r. The algorithm continues by altering r to progressively smaller sizes and counting N_r . The slope of the line fitted through the plot of log (1/ r) against log (N_r) is the fractal, or box-counting, dimension of the bovine muzzle image region under investigation

IV. EXPERIMENTAL RESULT

A. *Database*

Muzzle database is the first challenge that we face when we start this research because of insufficiency muzzle printed database. Our muzzle database consists of 53 different cattle muzzle, each cattle has twenty captured image, this database for a real time cattle which collected by Dr. Hamdi Mahmoud. A sample of four different images to three muzzle captured image is shown in the following figure.

A sample of muzzle printed images from live animals. This figure represented muzzle print images have been taken from three different animals.

B. *Histogram equalization*

Histogram equalization widely employed as enhancing algorithm. We can see that the image's contrast has been improved. The original histogram has been stretched along the full range of gray values, as we can see in the histogram equalization in Fig. 1.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

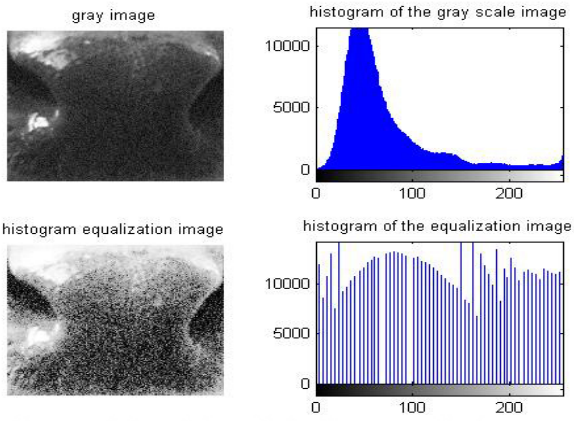


Fig. 1. muzzle image before and after histogram equalization

By compare histogram to three different images to the same bovines we found that histogram is symmetry as in the fig. 2.

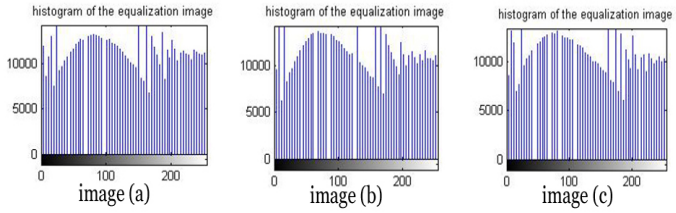


Fig. 2. Three different image to the same bovine muzzle

By compare histogram to another three different image to the same bovines we found that histogram is symmetry as in the fig.3.

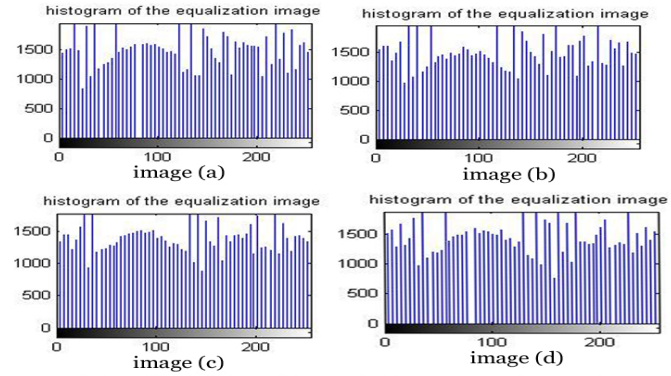


Fig. 3. Four different image to the same bovine muzzle

The histogram to different muzzle is dissimilar as in fig. 4.

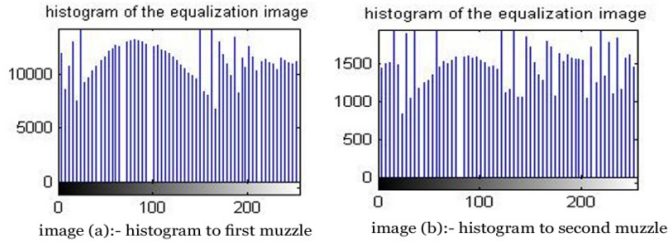


Fig. 4. histogram to two diferent muzzle image

In image processing the histogram equalization is the process which shows the appearance of each intensity value in muzzle image. Histogram graph show number of pixels at each different intensity value. For example if the image has 9-bit gray scale this mean that there are found 512 different intensities value, so the histogram graph show 512 numbers which show pixels distribution among each gray scale values [21]. Histogram equalization increase image contrast because it specify the intensity value of the input image pixels, so histogram aim is that the output graph contain a uniform distribution of intensities. Histogram equalization method increases global image contrast [22].

C. Mathematical morphology filtering (MM)

Opening operation of *A* by *B* obtained by erosion of *A* by *B* then dilation of the resulting muzzle image by *B*. Return to fig. 5 that's contain the result image to muzzle after opening operation.

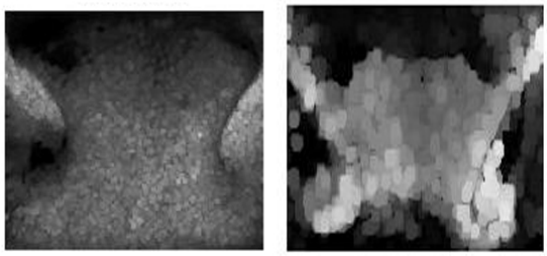


Fig. 5. opening operation on different muzzle

The output muzzle image that is in fig. 5. is used as input image in close operation. Closing operation of *A* by *B* obtained by dilation of *A* by *B* then erosion of the resulting muzzle image by *B*. The result image illustrated in fig. 6.

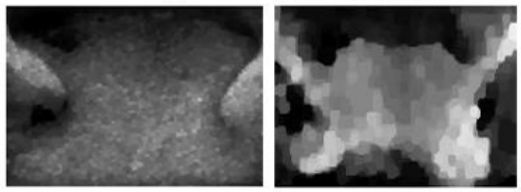


Fig. 6. close operation for two different muzzle

After image preprocessing operations histogram equalization (HQ) and mathematical morphology filtering (MM) low contrast muzzle transformed to high contrast and noise removed respectively. Now the muzzle image become ready to the second step that is texture feature extraction.

D. Texture feature extraction using box counting method

The implementation of box-counting in different image to the same bovine result to the same result return to fig. 7. That show 2D box- counting to four different image to on bovine muzzle.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

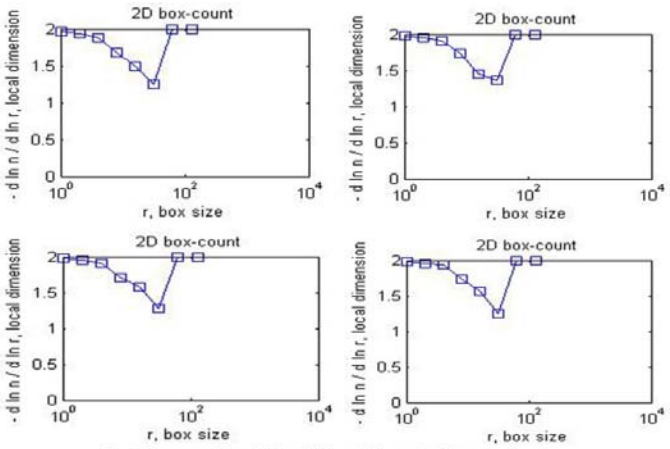


Fig. 7. box-counting to four different image to the same bovien

Fig. 8. Show another result to different bovine muzzle

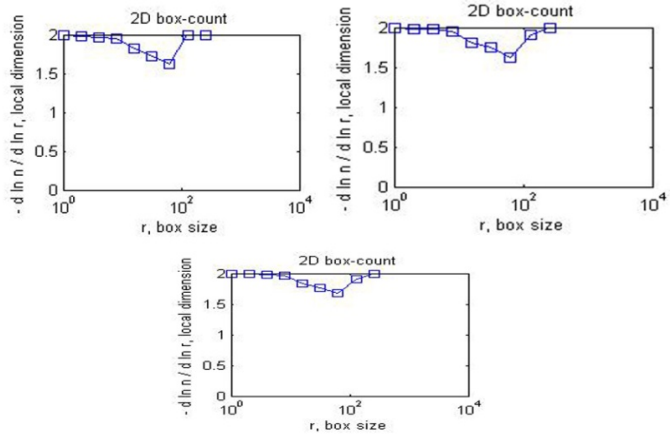
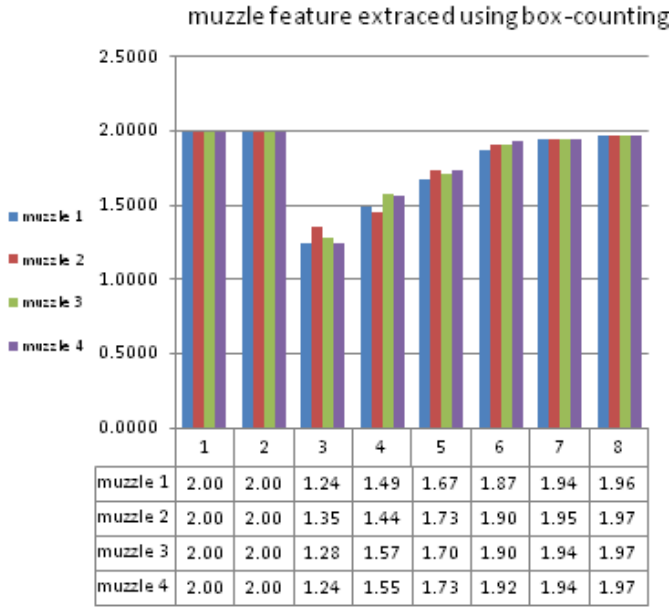


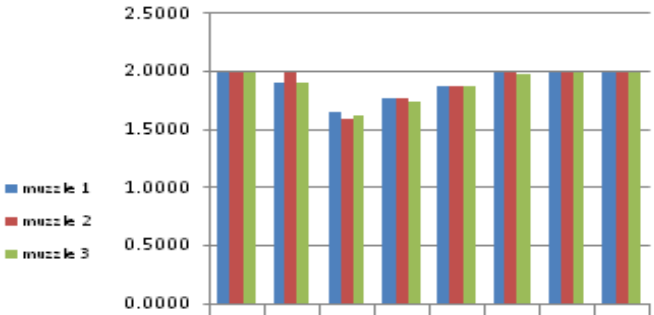
Fig. 8. box-counting to three different image to the same bovien

Previous after implementing box-counting algorithm on different muzzle image and each muzzle has different image the experimental result show the high similarity between the different image to the same bovine muzzle as in the following chart.



	1	2	3	4	5	6	7	8
muzzle 1	2.00	2.00	1.24	1.49	1.67	1.87	1.94	1.96
muzzle 2	2.00	2.00	1.35	1.44	1.73	1.90	1.95	1.97
muzzle 3	2.00	2.00	1.28	1.57	1.70	1.90	1.94	1.97
muzzle 4	2.00	2.00	1.24	1.55	1.73	1.92	1.94	1.97

Another three different image to the same bovine.



	1	2	3	4	5	6	7	8
muzzle 1	2.00	1.90	1.64	1.77	1.88	1.98	1.99	1.99
muzzle 2	2.00	2.00	1.58	1.77	1.88	1.99	1.99	1.99
muzzle 3	2.00	1.90	1.61	1.74	1.87	1.98	1.99	1.99

The fractal dimension to four images to one bovine which has histogram appears in fig. 3. And box counting result in fig. 7 is approximately equal.

Fractal dimension, FD =	**1.6827 +/- 0.32645**
Fractal dimension, FD =	**1.7086 +/- 0.30032**
Fractal dimension, FD =	**1.7132 +/- 0.30303**
Fractal dimension, FD =	**1.7086 +/- 0.31821**

The fractal dimension to three image to another one bovine which has histogram appear in fig. 4. And box counting result in fig. 8 is approximately equal.

Fractal dimension, FD =	**1.8424 +/- 0.13487**
Fractal dimension, FD =	**1.8477 +/- 0.17476**
Fractal dimension, FD =	**1.8289 +/- 0.15011**

So we can use this result in muzzle image classification and identification.

V. Conclusion and Future Work

This paper has presented feature extraction to database consists of muzzle image. First, the statistical representation preprocessing techniques (Histogram equalization and mathematical morphology filtering) have been used in order to increase the contrast of each image and remove image noise. Then, box-counting algorithm has been used to extract the feature vector to each muzzle case. Simulation results have shown that the statistical representations for different images of the same muzzle are correct. The disadvantage of the statistical representation is that in case of lager amount of data (image), we need more intelligent techniques to give us accurate results. So, in the future work we may use big data algorithms together with intelligent soft comporting techniques.

References

[1] Fitzgerald, L. (2004): "The efficacy of muzzle recognition as a method for identification of cattle". Thesis of Masters of Science in Engineering Technology. Bio-systems Engineering. University College Dublin, Ireland.
[2] Barron, U. G. (2005): "Muzzle pattern as a biometric identifier for cattle. Development of a protocol for biometric-based animal

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

tracking and tracing". This research is supported by the Irish Government under the National Development Plan 2000-2006.
[3] Baranov, A. S., Graml, R., Pirchner, F., and Schmid, D. O. (1993): "Breed differences and intra-breed genetic variability of dermatoglyphic pattern of cattle". J. Anim. Breed Genet., 110:385-392.
[4] Minagawa, H., Fujimura, T., Ichiyanagi, M., and Tanaka, K. (2002): "Identification of beef cattle by analyzing images of their muzzle patterns lifted on paper". Publications of the Japanese Society of Agricultural Informatics, 8, 596-600.
[5] Liu, L., Gangyao Kuang, G. (2009): "Texture Feature Extraction Method". Chinese Image and Graphics Learning Journal, 14(4), 622-634.
[6] Miljkovi´c, O. (2009): "Image Pre-processing Tool". Kragujevac J. Math. 32 97-107.
[7] Červinka, O., Provazni'k. I. (2007): "Pre-processing for Segmentation of Computer Tomography Images". The Faculty of Electrical Engineering and Communication Brno University of Technology,Department of Biomedical Engineering.
[8] ANITHA, S., RADHA, V. (2010): "Comparison of Image Preprocessing Techniques for Textile Texture Images". International Journal of Engineering Science and Technology, Vol. 2(12), 7619-7625.
[9] Krutsch, R., Tenorio, D. (2011): " Histogram Equalization ". Microcontroller Solutions Group, Document Number: AN4318, Rev. 0, June, Freescale Semiconductor, Inc.
[10] Yeganeh, H., Ziaei, A., Rezaie, A. (2008): "A Novel Approach for Contrast Enhancement Based on Histogram Equalization".978-1-4244-1692-9/08/$25.00©IEEE. Proceedings of the International Conference on Computer and Communication Engineering.
[11] Hong, SH. And Huidong, D. (2012):" Fractal Dimension Applied in Texture Feature Extraction in X-ray Chest Image Retrieval". Proceeding of the IEEE International Conference on Information and Automation Shenyang, China, June: 978-1-4673 2237-9/12/$31.00.
[12] Serra, J. (1982): "Image analysis and mathematical morphology", Academic Press, London.
[13] Droogenbroeck, M., Buckley, M. (2005): " Morphological erosions and openings: Fast algorithms based on anchors". Fast Algorithms Based on Anchors. Journal of MatheMathematical Imaging and Vision.
[14] Ander G.R.Balan, Agma G.M.Traina, Caetano Traina Jr.1, Paulo M. Azevedo-Marques. (2005): "Fractal Analysis of Image Textures for Indexing and Retrival by Content". Proceedings of the 18th IEEE Symposium on Computer-Based Medical Systems.
[15] J. J. Gangepain, C. Roques-Carmes. (1986) "Fractal approach to two dimensional and three dimensional surface roughness". Wear, (109): 119-126.
[16] N. Sarker, B. B. Chauduri. (1992): "An efficient approach to estimate fractal dimension of texture images". Pattern Recognition, 25(9), 1035-1041.
[17] N. Sarker, B. B. Chauduri. (1994): "An efficient box-counting approach to compute fractal dimension of image". IEEE Trans. Syst. Man Cybernet. 24: 115-120.
[18] Theeta-Umpon, Nipon. (2002): "Fractal dimension estimation using modified differential box-counting and its application to MSTAR target classification". Proceedings of the IEEE International Conference on System, Man and Cybernetics, 2: 537 541.
[19] Chen, Wen-Shiung, Yuan, Shang-Yuan Hsich, Chih-Ming. (2003): "Two algorithms to estimate fractal dimension of gray-level images". Optical Engineering, 42(8): 2452- 2464.
[20] Esteller, R., Vachtsevanos, G., Echauz, J., Litt, B. (2001): "A Comparison of Waveform Fractal Dimension Algorithms", IEEE Trans. On Circuits and Systems -I: Fundamental Theory and Applications, Vol.48, No. 2, pp 177 183 Feb.
[21] Rafael C. Gonzalez, Richard E. Woods,"Digital Image Processing Using MATLAB", Pearson Education, Inc.
[22] Manvi, Chauhan, R. S., Singh, M. (2012): "image contrast using histogram equalization". International Journal of Computing & Business Research, ISSN (Online): 2229-6166.
[23] Hazem M. El-Bakry, "An Efficient Algorithm for Pattern Detection using Combined Classifiers and Data Fusion," Information Fusion Journal, vol. 11, issue 2, April 2010, pp. 133-148.
[24] Alaa M. Riad, Ahmed Atwan, Hazem M. El-Bakry, Reham R. Mostafa, Hamdy K. Elminir, and Nikos Mastorakis "A New Approach for Segmentation of Brain MR Image, " Proc. of ENVIRONMENT, MEDICINE and HEALTH SCIENCES (EMEH'10), Penang, Malaysia, March 23-25, 2010, pp. 74-83.
[25] Hazem M. El-Bakry, "A Novel High Speed Neural Model for Fast Pattern Recognition," Soft Computing Journal, vol. 14, no. 6, 2010, pp. 647-666.
[26] Hazem M. El-Bakry, Alaa M. Riad, Ahmed Atwan, Sameh Abd El-Ghany, and Nikos Mastorakis "A New Automated Information Retrieval System by using Intelligent Mobile Agent, " Proc. of Recent Advances in Artificial Intelligence, Koweledge Engineering and Databases, Cambridge, UK, February 20-22, 2010, pp. 339-351.
[27] Hazem M. El-Bakry, "New Fast Principal Component Analysis For Real-Time Face Detection," MG&V Journal, vol. 18, no.4, 2009, pp. 405-426.
[28] Hazem M. El-Bakry, and Nikos Mastorakis, "Fast Image Matching on Web Pages," WSEAS Transactions on Signal Processing, issue 4, vol. 5, June 2009, pp. 157-166.
[28] Hazem M. El-Bakry, "A New Neural Design for Faster Pattern Detection Using Cross Correlation and Matrix Decomposition," Neural Network World journal, 2009, vol. 19, no. 2, pp. 131-164.
[30] Alaa M. Riad, Ahmed Atwan, Hazem M. El-Bakry, Sameh Abd El-Ghany and Nikos Mastorakis, "An Intelligent Distributed Algorithm for Efficient Web Image Retrieval," International Journal of Communications, issue 3, vol. 3, 2009, pp. 63-76.
[31] Hazem M. El-Bakry, and Nikos Mastorakis "Ear Recognition by Using Neural Networks " Proc. of APPLIED COMPUTING CONFERENCE 2009 (ACC '09), Vouliagmeni Beach, Athens, Greece, September 28-30, 2009, pp.770 - 804.
[32] Hazem M. El-Bakry, and Nikos Mastorakis "Fast Human Motion Tracking by using High Speed Neural Networks " Proc. of 9th WSEAS International Conference on SIGNAL, SPEECH AND IMAGE PROCESSING (SSIP '09), Budapest, Hungry, September 3-5, 2009, pp. 221-240.
[33] Hazem M. El-Bakry, "New Faster Normalized Neural Networks for Sub-Matrix Detection using Cross Correlation in the Frequency Domain and Matrix Decomposition," Applied Soft Computing journal, vol. 8, issue 2, March 2008, pp. 1131-1149.
[34] Hazem M. El-Bakry, and Nikos Mastorakis, "A New Technique for Detecting Dental Diseases by using High Speed Artificial Neural Network," WSEAS Transactions on Computers, Issue 12, vol. 7, December 2008, pp. 1977-1987.
[35] Hazem M. El-Bakry, and Nikos Mastorakis, " An Effective Method for Detecting Dental Diseases by using Fast Neural Networks," WSEAS Transactions on Biology and Biomedicine, issue 11, vol. 5, November 2008, pp. 293-301.
[36] Hazem M. El-Bakry, and Nikos Mastorakis, " A New Technique for Detecting Dental Diseases by using High Speed Neuro-Computers, " European computing Conf. (ECC '08), Malta, September 11-13, 2008, pp. 432-440.
[37] Hazem M. El-Bakry, and Nikos Mastorakis "New Fast Normalized Neural Networks for Pattern Detection," Image and Vision Computing Journal, vol. 25, issue 11, 2007, pp. 1767-1784.
[38] Hazem M. El-Bakry, and Nikos Mastorakis, "A New Approach for Fast Face Detection," WSEAS Transactions on Information Science and Applications, issue 9, vol. 3, September 2006, pp. 1725-1730.
[39] Hazem M. El-Bakry, and Qiangfu Zhao, "Fast Normalized Neural Processors For Pattern Detection Based on Cross Correlation Implemented in the Frequency Domain," Journal of Research and Practice in Information Technology, Vol. 38, No.2, May 2006, pp. 151-170.
[40] Hazem M. El-Bakry, "New Fast Principal Component Analysis for Face Detection," Journal of Advanced Computational Intelligence and Intelligent Informatics, vol.11, no.2, 2007, pp. 195-201.
[41] Hazem M. El-Bakry, "Face detection using fast neural networks and image decomposition," Neurocomputing Journal, vol. 48, October 2002, pp. 1039-1046.
[42] Hazem M. El-Bakry, "Human Iris Detection Using Fast Cooperative Modular Neural Nets and Image Decomposition," Machine Graphics & Vision Journal (MG&V), vol. 11, no. 4, 2002, pp. 498-512.
[43] Hazem El-Bakry, "Fast Face Detection Using Neural Networks and Image Decomposition," Lecture Notes in Computer Science, Springer, vol. 2252, December, 2001, pp.205-215.
[44] Hazem M. El-Bakry "A Rotation Invariant Algorithm for Recognition," Lecture Notes in Computer Science, Springer, vol. 2206, October 2001, pp. 284-290.
[45] Hazem M. El-Bakry "Fast Iris Detection for Personal Verification Using Modular Neural Networks," Lecture Notes in Computer Science, Springer, vol. 2206, October 2001, pp. 269-283.
[46] Hazem M. El-Bakry, "Automatic Human Face Recognition Using Modular Neural Networks," Machine Graphics & Vision Journal (MG&V), vol. 10, no. 1, 2001, pp. 47-73.

Title of Paper: Electricity Power Theft Detection Using Wireless Prepaid Meter.

1. Author Name: Ebole Alpha F.

Department Of Computer Science, Lagos State Polytechnic, Ikorodu Lagos – Nigeria.

(Laspotech)

Ikorodu, Nigeria.

2. Co – Author: Prof. N. Goga

University Of Groningen, The Netherland

Netherland.

ABSTRACT

Energy meters in Nigeria have dominantly been electromechanical in nature but are gradually being replaced by more sophisticated and accurate digital and electronic meters. Today, a high percentage of electricity revenue is lost to power theft, incorrect meter reading and billing, and reluctance of consumers towards paying electricity bills on time based on postpaid meter. Considerable amount of revenue losses can be reduced by using Prepaid Energy Meters. A prepaid energy meter enables power utilities to collect energy bills from the consumers prior to the usage of power by delivering only as much as what has been paid for. This research provides a prepaid energy meter behaving like a prepaid mobile phone. The meter contains a prepaid card similar to mobile SIM card. The prepaid card communicates with the power utility using mobile communication infrastructure. Once the prepaid card is out of balance, the consumer load is disconnected from the utility supply by the contactor. The power utility can recharge the prepaid card remotely through mobile communication based on customer requests or consumer purchasing recharge card. A prior billing is bound to do away with the problems of unpaid bills and human error in meter readings, thereby ensuring justified revenue for the utility. Over the past several years, smart cards have achieved a growing acceptance as a powerful tool for security, identification, and authorization. The increasing computational power placed on the chip along with advances in cryptography has made the smart card a very powerful tool for identification. The advent of multi-application smart card operating systems for both contact and contact less applications has put smart cards on the edge of information technology. The proposed system uses an IP-based controller for the prepaid meter and the load meter and the responsibility of Load meter is to provide a simple way of detecting electricity power theft without any human intervention. The Load meter would indicate exact building or location and distribution line on which unauthorized taping is done in real time. It would be time saving if distribution company personnel take reading by this wireless technique and also it would provide a digital record in case of any judicial dispute which will be use for comparative analysis between the prepaid meter. The idea is to maximize the profit margin of power utility company, efficient online control of the total amount of electricity consumed in a specific location and be able to detect when there is bypass by the user either by shoot- hunting without connecting the cable through the digital meter or parts of the equipment are connected through to the smart meter why high voltage equipment are bypassed.

KEYWORDS: Prepaid Meter, IP-Based Controller, Load Meter.

INTRODUCTION

The Generation, Transmission and Distribution (T&D) as well as supply of electricity involve huge operational losses. The magnitude of these losses is rising at an alarming rate in several countries. In order to identify illegal consumers of electricity in the view of enhancing the economy of utilities, efficiency and security of the grid, a new method of analyzing electricity consumption patterns of customers and identifying illegal consumers is proposed and realized. Nigeria electric power network operator, Power Holding Company of Nigeria (PHCN) has over the years being faced with the problem of revenue collection. This is mostly because electricity bills are sent to consumers after it has been consumed. Consumers are reluctant to pay electricity bills due to estimated bills and unreliable and irregularity power supply. The low reliability of electric power supplies has little or no impact on the network operator because whether there is power or not, the normal estimated monthly electricity bills are sent to consumers in the post-paid method. Therefore, the consumers suffer the cost of generating power for their individual usage and the cost of electricity that was never supplied by PHCN. Due to the huge debt owed by customers, the network operator introduced a cash collection policy called Revenue Cycle Management (RCM) that involves using private companies in the collection of monies owed. This seems not to yield the expected results; hence PHCN introduced the digital pre-paid meter in 2006 which operation is similar to the loading of recharge card in the Global System for Mobile communication handset. If power is available and the pre-paid meter is loaded with units, the loaded units decreases only when load is connected and stops when power fails.

In the last decade, smart cards evolved from basic memory cards to complex systems on chips with expanding processing power. This has opened the avenue to many applications such as financial transactions, e-commerce, physical access control, health, and transportation services. The smart card, an intelligent token, is a credit card sized plastic card embedded with an integrated circuit chip. It provides not only memory capacity, but computational capability as well. A smart card usually consists of a ROM or flash memory, EEPROM and a CPU. Access to data stored on the card is under the control of the smart card operating system. The card operating system not only makes the smart card secure for access control, but can also store a private key for a public key infrastructure system. Lately, the industry has come up with 32-bit smart card processors having more than 400Kbytes of EEPROM, and a memory management and protection unit serving as a hardware firewall. This hardware firewall enables secure separation of adjacent applications, as well as being the basis for secure downloading of applications. The self-containment of smart card makes it resistant to attack as it does not need to depend upon potentially vulnerable external resources. Because of this characteristic, smart cards are often used in several

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

applications which require strong security protection and authentication. In addition to information security, smart cards achieve greater physical security of services and equipment, because a smart card restricts access to all but authorized users. Furthermore, the smart card can be used as a credit/debit bank card which allows it to be used effectively in e-commerce applications. The multi-application smart card, along with the advent of open platform smart card operating systems, brings the only realistic option for managing multiple electronic transactions nowadays. It is a cost effective secure way to manage transactions electronically Manufacturers, issuers and users have recognized the value of one card that handles multi-applications. A multi-application card will be able to automatically update new services and existing applications, change and store user profiles for each application and be accepted by a range of devices-PC, POS, mobile phones. One of the most valuable applications is in using the smart card to buy energy. Domestic consumers could for instance buy energy, at a price based on their previous consumption pattern, from any supplier wherever and whenever they choose. When the customer wants to top up their electricity credit they visit a vending machine which uses the consumption data stored on their card to allocate a tariff and calculates how much energy to offer the consumer for their money. Recently, the portal technology has been playing an increasing role in computing. Service providers are rolling out portals to allow users to create customized web sites that display exactly the information on the Card and transformer. Corporations are rolling out portals to provide employees and business partner's customizable access to corporate information, including new feeds from external providers, or email, calendar and access to billing system, in addition to other web services. For web enabled energy services, and with the advent of home networking technology, power companies and service providers can provide value-added services delivered to the homes, like energy management, to generate additional revenue as well as to increase convenience and loyalty. In this research work, we propose a novel and simple prototype of a web enabled smart card based solution for controlling the consumption of electricity in a home environment, system that can calculate the total voltage consumption and the structure health condition of the transformer as well as the total voltage distributed by the transformer. Since the last decades of the past century, scientists, researchers and public people have been worried about energy conservation. People spend much more power than what they actually need and that results in a huge loss of energy. Moreover, the continuous increase in the universal energy prices has resulted in a huge economical loss. Thus we are proposing a prepaid electricity smart card based system so people can buy specific amount of energy to use it only when they need. People can register for this service and charge their accounts through the Internet. The proposed system is based on an IP-based controller called TINY, and a WATTNODE type power meter which interrupts the controller at a regular interval based on the consumption of electricity to update the balance based on a certain tariff. The power meter we used, interrupts the controller at a rate of 0.75Wph, so based on the particular tariff used and the amount

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

of power consumption needed, the correct amount of money to be loaded into the card can be easily calculated and programmed into the chip. The unique feature about this system is that the electric utility in the home environment can be accessed remotely from the supplier server due to the fact that the controller is IP-based, without the need for a PC on site, which reduces the cost of the system drastically. People now can buy electricity in advance, using the so-called prepaid electricity cards. The proposed prepaid smart card can also be used to manage electricity consumption in a hotel room, as well as accessing the room itself. Thus, people can consume only as much power as they really need. The main role of the smart card can be summarized as:

- Authenticating the user or log in
- Updating the balance in the card based on the given tariff and the electricity consumption profile of the user stored in the smart card. See Figure below for the proposed system.
- Automatic respond on customer report on any bypass.

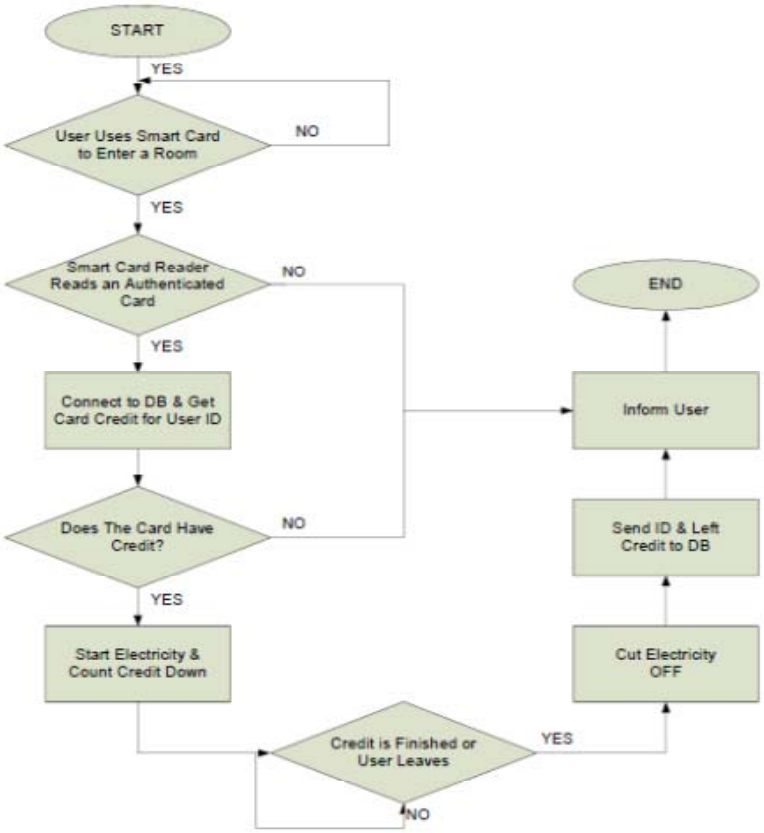


FIG 1. Flow Chart for Prepaid Electricity

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

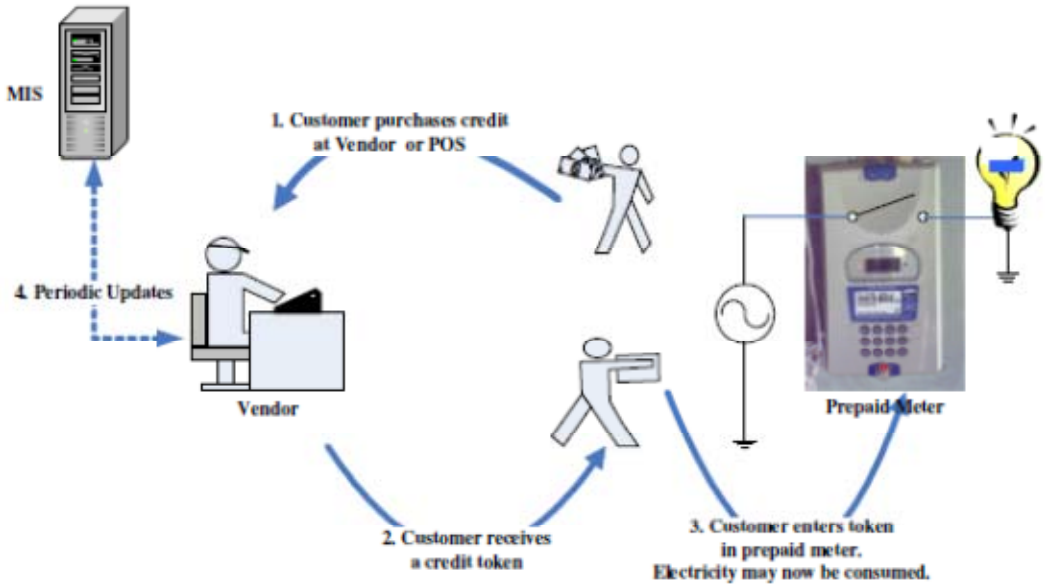


FIG. 2 Stage of Activities in prepaid Card.

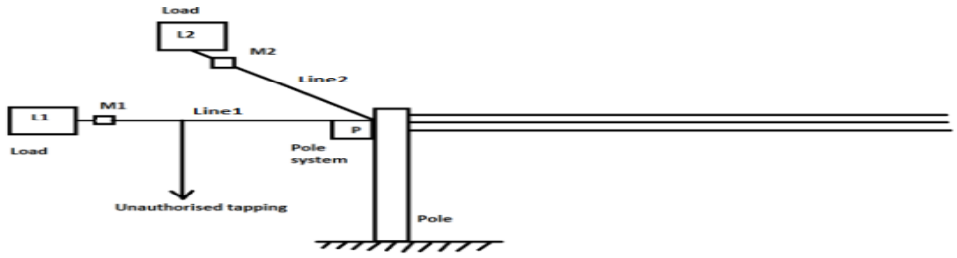


FIG 3. Conceptual diagram of Pole based system

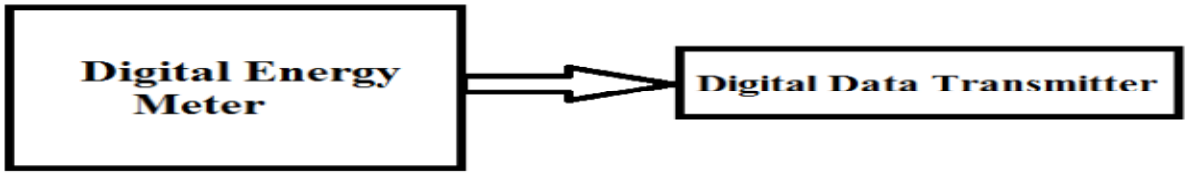


Fig 4 Load side energy meter

STATEMENT OF THE PROBLEM

Electric energy meters, the direct billing interface between utilities and consumers for long, have undergone several advancements in the last decade. The conventional electromechanical meters are being replaced by new electronic meters to improve accuracy in meter reading. Still, the Nigeria power sector faces a serious problem of low revenue collection for the actual electric energy supplied owing to energy

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

thefts through bypass from digital meter. One of the prime reasons is the traditional billing system which is inaccurate many times, slow, costly, and lack in flexibility as well as reliability. Therefore, attempts are being made to automate the billing systems, even though more accurate and faster meter readings have seen the light of day; bill payment is still based on an old procedure. They require an individual/agent to personally come down to customer place and note the meter readings and report the amount one has to pay to the household/office. But the demand for computing power at all levels of electronic systems is driving advancements in semiconductor chip technology. The AMR and power quality monitoring systems manufacturers are taking advantage of these advances and integrating them into new meters and instruments. The networking technologies are driven by the demand for interconnection of computer users worldwide. The AMR and power monitoring systems are using these advances to expand the monitoring systems. A Prepaid Energy Meter enables power utilities to collect electricity bills from the consumers prior to its consumption. The prepaid meter is not only limited to Automated Meter Reading [AMR] but is also attributed with prepaid recharging ability and information exchange with the utilities pertaining to customer's consumption details. But, there primary objective were not met due to energy theft by bypassing a digital prepayment meter, which is an economic lost to the Government.

AIM OF THE RESEARCH

A secure smart card based system for e-payment, implemented on prepaid electricity over the internet, was proposed. The smart card system has been designed and implemented successfully using a three tier model client-server system. The proposed system has the benefit of using a secure smart card to log in to the network, and control the amount of money needed to be spent for the required electricity consumption based on the user profile stored on the card and also to give an automatic report on an bypass of voltage through the means of shoot hunting or short circuited without the user connecting through the smart card or quick Load meter system design to transmit total voltage consume within a define specified location. The proposed system also has the unique feature of using an IP-based controller which provides remote access to prepaid meter and Load meter information within that particular location in other to ensure total consumption which link to the server without any additional cost.

OBJECTIVE OF THE RESEARCH

- To explore and investigate various electricity payment system
- To propose a model for IP Based smart card payment system.
- To evaluate the proposed Model as a solution to bypassing
- To design and implement these model as a Real time processing in solving the problem of bypassing.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- To implement a real time Load meter system use to transmit total voltage consume within a particular location

RESEARCH QUESTION

- Are these various methods of electricity billing system prevented fraud?
- Has the introduction of pre-paid meters aided revenue generation in Nigeria?
- What is the best method in solving the problem of bypassing?
- What is the means of identification of total voltage availability in the building?
- How can bypass be detected?

REVIEW OF RELATED LITERATURE.

Introduction

As deregulation takes hold, customer competition and care is gathering pace as the wave in the utility industry. And central to this, linking utility and customer, is the meter, whose role is becoming increasingly important with impact on all areas of the metering business from metering practice and metering technology to billing.

Metering according to Simpson (1996:14) is the process and methods of utilizing devices to measure the amount and direction of electrical energy/flow, particularly for end-use. " he also defined metering as " installation of equipment that makes it possible for a utility to determine the amount of electric power a particular customer has consumed. " electricity is provided to customers by wires, often called service drops, emerging from distribution transformers. These wires go into the electric meters that measure the quantity of electricity used (measured in kilowatt-hours.)

Meter

According to Austin (2002). "The meter is both a means of measuring energy supply and also a critical sales and marketing tool, which has a correlation with company's profitability." Meters are for correct measurement of electricity to ensure customers pay for their consumption while enabling utilities to charge based on what has been supplied. According to Leitner (1998:231), customers need value for the money spent in installing the meters; therefore, the meter which gives value for the money must be functioning properly at all times. The meter is typically located where the utility hands off the delivery of electricity to the customer. Generally the customer is responsible for purchasing and maintenance

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

equipment past this point. Thus there is need for proper management and maintenance of the meters for effectiveness and efficiency in the prepayment Metering System. Utility business and operational services should no longer be segmented- for example, linking energy management tools (such as load profiling, monitoring and control and demand response management) to a metering and customer information system (CIS) will encourage customer loyalty, reduce demand and assist in managing costs" (Metering Billing and CRM/CIS), 17-19 February 2004, Kuala Lupur, Malaysia.

Metering as a System

The meter is key tool in any utility requiring efficient operation and maintenance as it links the utility with customers (Kettless 2004:56). Thus, the General System Theory (Chadwick 1978) has been adopted as the conceptual framework for the study. A prepayment Metering System has viewed as a system with many interrelated sub-systems. the General System Theory is one major theory at the root modern scientific approach to management Chadwick (1978:36) defines a system as " a set of objects together with relationships between the objects and between their attributes," while Cole (1995) looks at it as an interrelated set of activities which enables inputs to be converted into outputs. Systems may be closed or open. Closed systems are those which for practical purpose, are completely self-regulating and thus not interact with their environment. Therefore, in the context of this study, a prepayment metering system cannot be closed as it relies on inputs from the community where it is stimulated for its survival. In this regard, Cole (1995:70) defines an open system as that which interacts with its community, on which it relies for obtaining essential inputs and for the discharge of system output. The inputs include people, materials, information, and finance, which are organized and activated so as to convert human skills and materials into products, services and other outputs that are discharge into the environment. The most important element of an open system is therefore, their inter-dependence on the community, which many are relatively stable or relatively uncertain at a particular point, (Cole 1995:71).

According to Clelland (1968:15), the management task of integrating various elements in the system is of paramount importance and this can only be effectively accomplished if the manager adopts the General Systems approach to the system he is managing. The system concept to prepayment metering in utilities is, therefore, a simple recognition that a prepayment metering is a system made up of sub- systems or the Master station, meter and the vending machine, each of which has its goals to achieve. In other words the meter record how much electricity has been consumed by the customer from the total produced by the utility while the master station ensures the customer has the correct amount of electricity sold to him through the vending machine and administers the whole system. "The boundaries between these sub-systems called interfaces may be external or internal." (Cole 1995:72) Consequently, in a system, some sub-systems have to deal with the inputs and the output for the system to work consistently at the external

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

boundary e.g. meter reading, billing customers and distribution of bills and so forth. On the other hand, other sub-systems deal with consistent provision of services to others in the system at the internal boundaries e.g. human resources, management and accounts.

Prepayment Metering System

Prepayment Metering is a well established technology being introduced by more and more utility companies. According to Keltless (2004), "a Prepayment Metering System is a system where a customer pays for energy before using it." A Prepayment Metering System according to Kettless (2004:105), basically comprises a system master station (which is a computer that operates and administers the whole system), a vending machine (where customers buy their electricity) and prepayment energy meters (or dispensers, which dispenses the electricity to the customer). This meter has an interface to the customer for managing the transfer of credit and to display the meter and credit status. In this study, the benefits and problems of the Prepayment Metering System can only be assessed by looking at various subsystems as a whole and seeking to understand and measure the effectiveness of the system. Prepayment metering systems are basically categorized as either one way or two-way, referring to the flow of information between the vending machine and the meter.

In the one-way system the information flows only in one direction, from the vending machine to the meter. This system can either be addressable or non-addressable. The addressable system uses tokens that are personalized to one meter and therefore cannot be used to credit any other meter. In the two-way system, information flows in both directions. In this system the meter also returns to the vending machine, information such as peak demand, average daily consumption etc. The system inherently requires expensive microprocessor smart cards, a sophisticated system of networked computers and vending stations.

Historical Development of Metering

Up to the 1870s, electricity had little use beyond the telephone and telegraph. The earliest use of electricity for power was to operate stings of arc lamps connected in series. "Since the current was constant and the voltage required for each lamp was known, and all the lamps were controlled by one switch, it was adequate to measure only the time current flowed in the current (lamp-hours)" (Lamphier, 1925). However, after the invention of the incandescent lamp by Edison in 1879 and the subdivision of lighting circuits for individual control of lamps, it was no longer practical to measure lamp- hours, but this practice continued into the 1890s. In 1882 Edison started up his first electric company for incandescent illumination. Initially he started out with a per-lamp rate. This was unsatisfactory so he developed a chemical ampere-hour meter that consisted of a jar holding two Zinc plates connected across

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

a shunt in the customer's circuit. Each month the electrodes were weighed and the customer's bill was determined from the change in their weight. However, this meter was inefficient and error prone because it was difficult to attribute all the change in weight to the flow of current. Edison did also develop a motor- type meter but preferred the chemical meter because of his interest in chemistry. Once the transformer was commercially feasible, it helped make the present system of AC transmission and distribution possible since it had none of DC's drawbacks at the time (voltage drop in long lines and lack of an easy way to increase or decrease voltage). "There was one major obstacle, however: There was no meter to accurately record the usage of electricity on AC circuits." (Lamphier 1925)

In 1885 Galileo Ferraris of Turin, Italy made a key discovery that two of phase AC fields can make a solid armature rotate. This discovery spurred developments of induction-type motors as well as paving the way for the development of the induction type watt-hour meters.

In 1886 Professor Forbes of London, England came up with the first meter for use on AC circuit that used a heating element connected into the circuit, which operated a small windmill connected to a register. Unfortunately this meter was far too delicate for commercial use.

In April 1888 at Westinghouse, Shallenberger and an assistant were working on an AC arc lamp when a spring fell out and came to rest on a ledge inside the lamp. The assistant reached over and was going to put it back when Shallenberger noticed the spring had rotated. After he realized that the spring had rotated due to rotating electric fields in the lamp he seized the opportunity and designed an AC ampere-hour meter in just 3 weeks, and it went on the market 3 months later. Over 120,000 Shallenberger ampere-hour meters were sold over the next 10 years (Hammond 1941). Thomson introduced his recording wattmeter in 1889. This was the first true wan-hour meter, and it was an immediate commercial success, many utilities adopting it as their "standard" model. Although this meter was initially designed for use on AC circuits, it worked equally well with the DC circuits in use at the time. The introduction and rapid acceptance of induction-type watt-hour meters in the late 1890's relegated the use of this commutator-type meter to DC circuits. With the rapid growth of the electric industry by 1894, AC was now being used to run motors, and the existing ampere- hour meters and commutator-type watt-hour meter were unable to take into account varying voltages and low power factors on AC circuits. Several inventors worked to develop a new meter to meet this need, but Shallenberger hit on the most workable approach- a small induction motor with the voltage and current coils 90 degrees out of phase with each. "This concept was refined into the first commercially produced induction watt-hour. This model was one of the heaviest ever offered at 41 pounds and one of the most expensive of its time." (Hammond 1941). However, he did not construct instruments that would measure the full continuum between the two circuits of AC and DC.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Credit Metering

Credit Metering is the traditional way of metering. This involves installing a meter at the customer's premises. The meter records the number of units, usually in kilowatt- hour, consumed every time power is switched on. The meter is read usually once in a month to determine the number of units that have been consumed by a customer and based on that consumption the customer is billed. The customer only pays when the bill has been made and presented to him. This system gives the customer a leeway in terms of time in which to settle the bill.

Prepayment metering System in the United Kingdom

Technology such as electronic metering systems with more advanced features, new prepayment metering technologies, and sophisticated utility software packages provides utilities with reliable, cost-effective meter-to-operations centre infrastructure. The challenge from a utility management perspective is how to capitalize on the opportunities to increase revenue, decrease costs and improve customer satisfaction. It is about extending the utility business well beyond microprocessor-based electronic hardware and enabling the utility to introduce systems that realize significant cost savings, efficiency gains and revenue enhancements. Revenue collection is one of the core activities of any utility. This has traditionally been accomplished using conventional credit meters with regular meter reading, extension of credit to customers and normal credit collection mechanisms. But as utilities around the world are coming to grips with deregulation, there is an increasing need for them to review existing business processes so as to make them more cost effective and customer friendly (Leitner, 1998).

Kettless (2004) states that Prepayment metering has been in use in the United Kingdom for well over 70 years, and with over 3.9 million electricity consumers on prepayment metering alone. The UK is seen as the world focus for prepayment development. This is further borne out by the types of token-based prepayment systems that have been introduced and developed over the last few years for the UK, which are now being marketed worldwide. The system ranges from the use of magnetic cards, key-based facilities, smart cards and so on. "It is interesting, however, to look back at the roots of prepayment systems, both from engineering and a social point of view. Mention prepayment metering to most utility staff and it will immediately conjure up images of consumers with bad debts" (Kettless, 2004:104). The UK has a long history of the use of coin operated meters, which allow a customer to pay for his electricity as he consumes it. By the late 1970s there were growing problems with coin operated meters. Some of them were: They were unreliable, the average 'life' on circuit being typically-5 years before needing attention. Although the customer paid in advance, the cash stayed in his meter until collected; hence it was not true prepayment from the utility view point.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cash was stolen from meters during burglaries, leaving the customer responsible for replacing it (and some customers 'stole' from their own meter). A meter might typically contain in excess of 100 pounds between collections. Staff collecting cash were targeted by criminals in robberies, to the extent that some collections had to be carried out using armored vans.

The electricity industry therefore encouraged research into alternative methods whereby prepayment facilities could be given without involving cash at the customer premises. Papers from that time record trials of, for instance, plastic coins which were crushed after insertion into the meter, and magnetic card tickets being developed by London Transport for the Underground system. Developments accelerated in the mid 1980s when the Prime Minister- Margaret Thatcher, launched an anti crime initiative, which included the problems of theft related to coin operated meters. By then manufacturers were close! To offering commercially viable new meters, but it was still early days and the industry was cautious about making a commitment to replacing the over one million operated meters.

One reason for caution was the need for (and cost of) a network of vending machines to support the meter base. "Roll-out of new prepayment meters was helped by two major reports prepared by the Electricity Industry (EI) around 1988 - one covering card and the other key technologies. Both concluded, taking into account benefits from cash flow brought forward." (Price 2001 :62)

Austin (2002) states that the prepayment industry is in a process of continual evolution as newer technologies emerge which provide enhanced functionality and allow utilities to offer innovative value-added services. Great strides continue to be made in the measurement techniques of prepayment meters, providing utilities with richer engineering services such as power quality monitoring, consumption history, time of use and meter status information. The key to gaining the greatest return and efficiencies from this information is to implement two-way feedback between the meter and the management system. This can be done as part of the purchase cycle, whereby data is transferred from an intelligent token device such as a smart card, button or electronic token key. When," new token is purchased, the vending outlet downloads the feedback data. However, this method relies entirely on the customer's purchasing cycle, which may be month to month, and thus provides no immediacy for utilities. According to Austin (2002), the demand for more sophisticated meters creates a ripple effect, whereby the revenue management system - the nerve centre for successful prepayment solutions, as it records all consumer transactions -undergoes a process of continual improvement to meet the metering needs. Reports currently generated from the data-rich management system allow utilities to monitor items such as consumer purchase patterns, determine energy load requirements, reconcile to bulk metering devices, detect non-technical losses and plan the maintenance of their systems. Simpson (1996) states that, advances in metering and communications have meant that many utilities throughout the world are

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

turning to two way communications technology to provide better and more efficient services for their customers. A progressive solution using power line carrier communications has been tried by the Scottish Power using the Siemens Mains Master 2000 system. Scottish Power believe this trial to be a world first in providing an operating token less prepayment system using power line carrier technology without any other metering back up. The fact that there are now 3.9 million prepayment customers, as opposed to no more that 1.5 million coin meter customer at peak, partly indicates that the new systems provides better benefit to both customers and the utility and partly relates to their use for other reasons, supporting the reasoning that coin operated meters are an alternative to disconnection of those unable to pay their bills despite its own drawbacks. For example, credit customers found to have interfered with their meters so as to avoid payment may be required to have a prepayment meter fitted as a condition of continued supply. In addition the new meters are flexible as regards tariff and some 25% of meters installed support a two-rate heating tariff. "Two major studies - one initiated by the Regular himself - have concluded that there is high customer satisfaction (around 90%) with the systems and the budgeting flexibility they offer." (Dick 2003:153) The use of prepayment meters also simplifies accounts considerably, more particularly in those cases where the tenants are constantly changing; for possibly two or three accounts might have to be sent out per quarter, to say nothing about the difficulty on occasions of finding the 'leaving' consumer. The scope of the prepayment meter is, however, not confined to the poor man's dwelling. Its use in flats is gradually becoming more extended, and in furnished apartments, where the consumers are chiefly nomadic. It relieves the proprietor of all responsibility as regards the consumption, over which he has practically no control" (Ferns, 1938:64).

Electric energy meters, the direct billing interface between utilities and consumers for long, have undergone several advancements in the last decade. The conventional electromechanical meters are being replaced by new electronic meters to improve accuracy in meter reading. Still, the Nigeria power sector faces a serious problem of lean revenue collection for the actual electric energy supplied owing to energy thefts. One of the prime reasons is the traditional billing system which is inaccurate many times, slow, costly, and lack in flexibility as well as reliability (Devidas*et al*, 2010). Therefore, attempts are being made to automate the billing systems. Even though more accurate and faster meter readings have seen the light of day, bill payment is still based on an old procedure. They require an individual/agent to personally come down to customer place and note the meter readings and report the amount one has to pay to the household/office. But the demand for computing power at all levels of electronic systems is driving advancements in semiconductor chip technology. The AMR and power quality monitoring systems manufacturers are taking advantage of these advances and integrating them into new meters and instruments. The networking technologies are driven by the demand for interconnection of computer

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

user's worldwide (Chandler, 2005). The AMR and power monitoring systems are using these advances to expand the monitoring systems.

In the recent past, several techniques were proposed for detecting the location of direct tapping on a feeder or tampered energy meter and identifying illegal consumers. On a parallel track, some non-technical measures, such as inspection of customers with suspicious load profiles and campaigning against illegal consumption, were also implemented to control electricity theft. Some of the techniques (proposed worldwide) are described in this section. A good strategy for fighting corruption in utilities has to be developed, considering the political scenarios, business processes, management techniques, and technologies in metering and distribution monitoring, control and automation based on the geographic location. In addition to the non-technical measures presented earlier, regularization of agricultural connections needs to be done. All of the contracts for deployment and maintenance of the distribution sector must be outsourced based on the performance of the enterprise to which the bid will be awarded. In addition, in most countries, electricity theft is considered a serious offense and illegal usage in any form of unbilled energy belonging to a utility is punishable under law. Laws and policies are being enforced such that political leaders do not protect corrupt employees and illegal consumers responsible for theft. A constituency has been proposed to be created through effective communication with the important stakeholders, institutionalization of new business processes that adopt modern technology, and improvisation of management information systems. Periodic inspection of illegal connections involves a lot of labor and strain for vigilant officials. The shunts detecting equipment proposed are time efficient and help in the detection of electricity theft in underground distribution cables. Revenue Assurance and Audit Process (RAAP) is composed of macro-functions to detect and analyze revenues involved in illegal consumption of electricity. Also, Mano R. *et al.* suggests proper design and implementation of rules in the investigation of illegal consumers. RAAP is targeted at improving the revenues for the utility by reducing commercial losses at about 20% each year. In India, the Electricity Act of 2003 has made electricity theft a punishable offence and gave full freedom to vigilance officials to inspect and detect illegal consumers. In Pakistan, Karachi Electric Supply Company (KESC) has obtained a fatwa or decree, from Islamic scholars, declaring that illegal consumption of electricity is a sin. On the other hand, teams are arranged for inspection and detection of illegal consumers of electricity, and their reward depends on the number of cases they inspect. Such incentives are proportional to the total number of illegal consumption cases they detect. Several technical measures were also implemented in order to detect and help utilities in their battle against NTL.

Installation of a prepaid energy meter can be a solution to monitor the distribution system and control electricity theft. Location of electricity theft on a distribution feeder can be detected based on the values

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

of the phase angle and impedance of the transmission lines at two different operating frequencies respectively. Bandim C.J. *et al.* proposed utilization of a central observer meter at secondary terminals of distribution transformer. The value of energy read by the central observer meter is compared with the sum of energy consumption values read by all energy meters in range. These two values of the current are compared to estimate the total electricity that is being consumed illegally. Vigilant Energy Metering System (VEMS) is a proposed energy metering system that can fight electricity theft. It has the ability to collect, transfer and process data between other energy meters, local station and base station. It also identifies probable locations of theft and helps the utilities to control theft. A remote billing system can also be developed modifying this model. Illegal consumption of electricity can be detected by using a remote check meter based on the amount of losses and time stamp of the check meter. This method is implemented before inspecting the illegal consumers personally by the vigilance officials, based on the data at the proper frequency of the consumer measurements. A microcontroller based energy meter proposed by Jamil M. *et al.*, gives utilities the ability to monitor and control the power supply of its spatially distributed consumers. This meter acts as a check meter that helps detect meters that have been tampered. In addition, e-metering systems can collect and process data, as well as detect abnormalities in load profiles indicating electricity theft.

Nagi J. *et al.* proposed a novel approach of using Genetic Algorithm-Support Vector Machines (GA-SVM) for detecting illegal consumption of electricity. Load consumption data of all the households is collected, and data mining techniques are used to filter and group these customers before detecting illegal consumption. Customers are grouped into different classes based on the extent of the abnormality in load profile and customers with high probability of theft are personally inspected. The Extreme Learning Machine (ELM) approach is used to evaluate abnormal load behavior indicating electricity theft based on a load-profile evaluation. Nizar A.H. and Dong Z.Y. used online sequential-ELM (OS-ELM) algorithms in detecting and grouping the load profiles to reduce.

A Prepaid Energy Meter enables power utilities to collect electricity bills from the consumers prior to its consumption. The prepaid meter is not only limited to Automated Meter Reading [AMR] but is also attributed with prepaid recharging ability and information exchange with the utilities pertaining to customer's consumption details. The idea of prepaid metering will be very important for the new research fields of Micro-grid and Smart Grid and is an inevitable step in making any grid smarter than it is now. Literature has witnessed quite an amount of work in this area. The use of electronic token prepayment metering has been widely used in UK for customers with poor record of payment (Southgate *et al*, 1996). A paper suggests a design of a system which can be used for data transmission between the personal computer and smart card. The device will transmit the data in half duplex mode (Kwan *et al*, 2002). The

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

system designed in this project can be used to develop more complex system where a smart card can be used to several applications including prepayment. Another paper features a 3-tier smart card secure solution for a novel prepaid electricity system. It uses an IP-based controller in addition to a power meter, providing efficient online control of the amount of electricity consumed by the user (Raad*et al*, 2007). Prepaid meters can also make use of state of art technologies like WiMAX owing to the idea of centralized accounting, monitoring and charging. It brings telecommunication to the core of its activities to support more Smart Grid applications such as Demand Response and Plug-in electric vehicles (Khan *et al*, 2007). Prepayment polyphone electricity metering systems have also been developed consisting of local prepayment and a card reader based energy meter (Ling *et al*, 2010). In this paper, we have attempted to initiate a different idea of using mobile communication to remotely recharge as well as bill the consumer's energy consumption. A prepaid card capable of communicating with power utility using mobile communication is attached to the energy meter.

A discussion of smart metering is often accompanied by a good deal of confusion about purpose and functionality, so it is necessary to start with definitions. To begin with a basic definition, 'smart' meters are primarily 'non-dumb', i.e. they communicate electronically, as: advanced meters that identify consumption in more detail than conventional meters and communicate via a network back to the utility for monitoring and billing purposes. (Climate Group, 2008, p. 85) It is not always necessary to replace a meter in order to achieve smartness: a 'dumb' meter can be 'smarted' by retrofitting it with communications capability and this is a less expensive option, for comparable specification. (Dimitropoulos (2007) gives a useful appraisal of costs and benefits of the equipment and rollout options open to UK utilities.) Taking the definition a little further, the literature shows general agreement that a fully smart meter is one that can measure and store data at specified intervals and act as a node for two-way communications between supplier and consumer and automated meter management (AMM). This allows for a radical change in customer–utility relations, with the possibility of remote disconnection and reconnection, remote change of tariff, and remote change in 'contractual power' (the peak electrical demand allowed for an individual customer, a familiar concept in Italy and France, for example). Simpler versions of communicating meters, usually referred to as 'advanced' rather than 'smart', have one-way communications only, from customer to utility. These are referred to as automated meter reading (AMR) meters, and have been used by industrial and commercial customers for many years, typically measuring consumption at half-hourly intervals for electricity, hourly for gas (Owen and Ward, 2006). They ensure accurate billing, make supplier switching more straightforward, and detect fraud more easily than standard credit meters. The term 'advanced metering infrastructure' (AMI) refers to the system of meters and associated communications. AMI offers accurate, fraud-resistant measurement (e.g. it tells the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

supplier when usage is suspiciously high or low, or when there is evidence of tampering), and improved information flows to enable demand response – the management of demand in relation to prevailing supply conditions (Batlle and Rodilla, 2008). It allows for communication hubs that can be used for the remote control of electrical appliances, in order to optimize network operation and the use of intermittent renewable supply. And it offers the prospect of integrated metering and recording for consumption and on-site generation. The most ambitious form of AMI, the 'smart grid', is planned to carry out load control at high resolution (the remote control of individual appliances from second to second), in order to cope with fluctuations in supply as well as demand. This is expected to become increasingly necessary as more intermittent renewable generation comes on stream (for an overview of the scope of smart grids, see European Commission, 2006a). Smart grids are still in the early pilot stage. A further definitional twist, but an essential one for this paper, comes from the separate development of electronic consumption displays, or in-home displays. These are widely (but misleadingly) known as 'smart meters'. Most display electricity usage, with a few also showing gas and water consumption. While many models are designed to operate with conventional meters, by sending signals to a display panel from a transponder attached to the meter tail, some recent models can operate with smart meters, showing accurate data that coincide with billing information.

TYPES OF PREPAYMENT METERS

Electromechanical prepayment meters in general consist of two parts. These are the integrating (Kwh) meter which is usually a standard meter made by the manufacturer to operate on the type of circuit concerned and the prepayment mechanism. This mechanism is subject to considerable variation.

Fixed charge collector - Hand-Reset Type

This is the simplest form of prepayment metering, consisting of the meter and a switch. At each visit the Meter Reader removes the money and trips the meter's switch. The consumer then re-closes the switch by inserting the requisite amount of cash.

Fixed charge collector - Time Switch Type

In this type of meter the tripping of the switch is performed by an electrically driven clock mechanism. The advantage with this meter is that it allows more frequent operations than the hand-operated type, and thus needs less amount of money each time to close the switch.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Flat rate tariff meter

In one form or another, this type of meter is the most commonly used? Turning the coin knob in this type of meter after the insertion of a coin in the slot advances a mechanical credit register the appropriate amount, and also closes the switch if it is not already closed. The coin is also registered on a counter which indicates the total number of coins inserted since the meter's installation. As the meter registers energy consumption, a linked gearing arrangement causes the credit register to progress towards zero. When zero is reached a tripping device operates and causes the switch to break the supply. A differential device prevents interference between the coin mechanism and the metering register. The coin register drives the credit counter upwards when coins are inserted, but with no effect on the meter register, while the meter register drives the credit counter downwards with no effect on the coin mechanism. The force required to open and close the switch is provided by a strong spring, which is charged by the consumer turning the coin knob and discharged by a trip mechanism on the credit register when it reaches zero. Meter manufacturers adopt one of two ways of allowing for unit price changes. In one design the gearing between the coin knob and the credit counter could be altered; in the other it is the gearing between the meter register and tile credit counter. Either way allows the number of units per coin to be adjusted to suit the tariff.

Two-part tariff - Fixed Rate Type

The next major development in prepayment metering is the Two Tariff-Fixed Rate type. This meter also incorporates a continuously running, constant speed motor. The motor is attached to the credit register via a differential gearing arrangement with a meter register. The mechanism used to calculate credit is the sum of the speeds of both the motor and the meter register through the differential gearing. The motor itself comprises the fixed charge collector. Running continuously through the differential gearing, it reduces the available credit in the meter even when energy is not being consumed. Because the motor runs at a constant speed, credit in the meter is reduced at a fixed rate per hour in addition to the number of units consumed, with a range of gears allowing for different fixed prices to be set.

Two-part tariff - Variable Rate Type

This meter has replaced the fixed charge motor with a second gearing system connected to the coin mechanism. Insertion of coins diverts a proportion of the money to the credit register and the rest to a fixed charge register, reducing the pre-set sum of money owed. When the fixed charge register reaches zero the associated gearing is disengaged from the coin mechanism, so that all future coins inserted are used only for consumption. The disadvantage with this type of meter is that it makes electricity seem very expensive during the period that the fixed charge is being repaid.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Double tariff, Current Change-Over Type

Here the load current passes through a relay in addition to the load switch and current coil. The relay is designed to change the gearing between the meter register and the credit register depending upon its position. The solenoid remains in the off position when load currents are low (e.g. lighting only) and the customer pays a rate that is low per unit. When the load current increases to a certain level the solenoid operates causing the gearing between the meter register and the credit register to change consequently reducing the consumer's charge per unit. This allows consumers to use heavy loads, such as irons, radiators and water heaters, at a reasonable cost, yet enabling the suppliers to obtain a fair price per unit when only lighting is being used.

Double tariff, time Change- Over Type

Similar in operation to the current changeover meter, this meter employs a clock mechanism to change the gearing between the meter register and the credit register at certain fixed times of the day or night. Suppliers can thus offer their consumers low rates per unit at night and other off-peak periods. Consumers thus benefit from the lower unit prices for their consumption, whilst suppliers benefit from improved load factors. Electrolytic Prepayment Meter.

It consists of a glass cell or jar containing a quantity of copper nitrate solution and a fixed plate of copper acting as a cathode. The anode is provided by a strip of copper wound round a bobbin, which is fed a short length at a time into the electrolyte by the insertion of coins. The consumer's load (up to 4 amperes) passes through the cathode, anode and electrolyte, which results in the anode being dissolved and the copper being deposited on the cathode. Eventually, the anode would dissolve sufficiently to break the circuit at the surface of the liquid and is only remade by the consumer inserting more coins, causing more copper strip to be immersed into the solution.

This meter suffers from a number of disadvantages. If overloaded, the copper deposited on the cathode has a tendency to become uneven and 'trees' often forms which eventually result in the electrolyte being short-circuited. The copper strip has to be replaced when used up and every two years or so the cathode has to be replaced and the electrolyte filtered and topped up.

REGULATORY ASPECTS OF SMART METERING

Commissioned by: National Association of Regulatory Utility Commissioners (NARUC)

Energy Regulators Regional Association (ERRA), Submitted by: David Balmert, Dr. Konstantin Petrov

KEMA International B.V., Utrechtseweg 310, 6812 AR Arnhem, the Netherlands. Bonn, 20 December 2010

Issue Paper: Smart Metering December 2010

ERRA Licensing/Competition Committee Members

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

ERRA FULL MEMBERS

Albania

Electricity Regulatory Authority, Mr. Elis Sala, Chief Sector for Licensing/Monitoring

Armenia

Public Service Regulatory Commission of Armenia, Commissioner Samvel Arabayjan

Azerbaijan

Tariff (Price) Council of the Republic of Azerbaijan, Ms. Nurlana Musaeva, Chief adviser, The Department of Monitoring, analysis and methodology, Methodology and information sector

Bosnia & Herzegovina

State Electricity Regulatory Commission, Mr. Saša Šćekić, Head of Licensing and Engineering Department

Chaiman of the Licensing/Competition Committee

Bulgaria

State Energy and Water Regulatory Commission, Commissioner Plamen Denchev

Croatia

Croatian Energy Regulatory Agency, Ms. Loridana Smoljanic, Head of the Legal Affairs and License Department

Estonia

Energy Regulatory Department of the Estonian Competition Authority, Ms. Riina Randma, Chief Specialist, Energy Regulatory Division

Georgia

Georgian National Energy Regulatory Commission, Commissioner Irma Kavtaradze

Hungary

Hungarian Energy Office, Ms. Zsuzsa Cseko, Analyst

Kazakhstan

Agency of the Republic of Kazakhstan for Regulation of Natural Monopolies, Ms. Kalila Tanatovna Kokkozova

Director of the Department on regulation in sphere electro- and power system

Kyrgyz Republic

National Agency for Antimonopoly Policy and Development of Competition, Mr. Timur Orozaliev, Head of Price and Tariff Department

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Latvia

Public Utilities Commission, Ms. Digna Eglite, Head of the Energy Regulation Division in the Legal Department

Lithuania

National Control Commission for Prices and Energy in Lithuania

Macedonia

Energy Regulatory Commission of the Republic of Macedonia, Mr. Strasho Zafirovski, Head of Technical/Energy Department

Moldova

National Energy Regulatory Agency, Mr. Gheorghe Lupan, Head of Regulation and Licensing Department

Mongolia

Energy Regulatory Authority of Mongolia, Mr. Monkhtulga Monkhoo, Head of the Licensing Department

Montenegro

Energy Regulatory Agency of the Republic of Montenegro, Mr. Miodrag Djekic, Presiding of the board

Poland

Energy Regulatory Authority, Ms. Malgorzata Wesolowska, Head of Unit at the Department of the Energy Enterprises

Romania

Romanian Energy Regulatory Authority, Commissioner Maria Manicuta, Director, Licensing and Network Access Department

Russian Federation

Federal Tariff Service, Mr. Igor Kasaev, Deputy Head of Legal Department

Serbia

Energy Agency of the Republic of Serbia, Mr. Nikola Radovanovic Senior Expert for System and Legal Affairs

Slovakia

Regulatory Office for Network Industries, Ms. Michaela Urickova, Department of Strategic Analysis

Turkey

Energy Market Regulatory Authority, Mr. Hulusi Kara, Group Head, Electricity Market Department

Ukraine

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

National Electricity Regulatory Commission of Ukraine, Mr. Yuriy Antonyuk, Head of Licensing Department

Bosnia and Herzegovina

Regulatory Commission for Electricity in Federation of Bosnia and Herzegovina, Mr. Ahmet Hukić, Head of Licensing and Technical Dept

Bosnia and Herzegovina

Regulatory Commission for Energy of Republika Srpska, Mr. Dragutin Petkovic, Head of Licensing Department

Romania

National Regulatory Authority for Municipal Services, Ms. Anca Cador Expert, Market Monitoring and Territory Consultancy Department

UNMIK Kosovo

Energy Regulatory Office, Mr. Afrim Ajvazi, Legal and Licensing Officer

The Hashemite Kingdom of Jordan

Electricity Regulatory Commission, Ms. Muna AlMusa, Licensing and Monitoring Engineer

Nigeria

Nigerian Electricity Regulatory Commission, Mrs. Olufunke Dinneh, Head, Legal, Licensing & Enforcement

Saudi Arabia

Electricity & Co-Generation Regulatory Authority, Mr. Abdulrahman M. Al-Mohizai, Director General, Licensing and Legal Affairs

United Arab Emirates

Regulation and Supervision Bureau, Mr. Andrew Walker, Director of Economic Regulation

United States of America

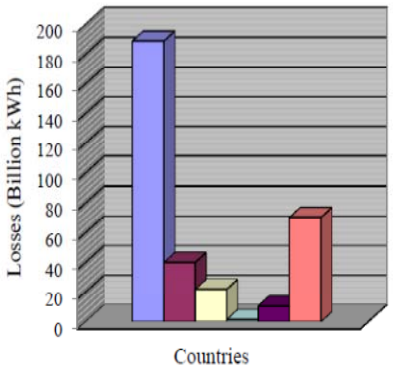
National Association of Regulatory Utility Commissioners, Ms. Kim Wissman, Deputy Director, Public Utilities Commission of Ohio

MOTIVATION

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Losses that occur during generation can be technically defined, but Transmission and Distribution (T&D) losses cannot be quantified completely from the sending-end information. Distribution losses in several countries have been reported to be over 30%. Substantial quantity of losses proves the involvement of Non-Technical Losses (NTL) in distribution. Total losses during T&D can be evaluated from the information like total load and the total energy billed, using established standards and formulae. In general, NTL are caused by the factors external to the power system. Electricity theft constitutes a major chunk of the NTL. Major forms of electricity theft include bypassing (illegal tapping of electricity from the feeder), tampering the energy meter, and physical methods to evade payment. Electricity theft can be defined as, using electricity from the utility without a contract or valid obligation to alter its measurement. Worldwide T&D losses are more than the total installed generation capacity of countries such as Germany, the UK, or France. It is estimated that utilities (worldwide) lose more than $25 Billion every year due to illegal consumption of electricity. For example, utilities in Nigeria lose around $4.5 billion every year due to electricity theft and a recovery of about 10% NTL can conserve about 83,000 GWh of electric power annually. In Pennsylvania, PPL, a utility reports an increase in electricity theft by 16% compared to 2013. It has also been identified that the illegal consumption of electricity by local business sector is increasing. Electricity worth approximately $14 million was pilfered in 2013 in the Houston area. In one year, Tampa Electric Company has seen a 20% rise in electricity theft, whereas, Progress Energy has seen an increase between 15 and 20%. Cost of nationwide electricity theft in USA is about $1–6 Billion every year. In Canada, BC Hydro reports that the electricity theft costs $100 million every year. Figure below shows overall T&D losses in several countries. It is evident that Billions of kWh of energy is being pilfered every year in several countries. Total losses incurred by utilities due to electricity theft are huge. As the impact of these losses is huge, it is essential to force the implementation of a mechanism that reduces NTL. Quality of the power generated, transmitted, and distributed, influences the 3 power system components, as well as customer appliances. Illegal consumption of electricity makes the estimation of overall load in real time very difficult. However, parameters involved in analyzing electricity theft include political, economic, criminal, and managerial. In addition, priorities in investment on implementation of new measures might also be prone to corruption.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500



Nigeria, Mexico, Pakistan, Dominican Republic, Colombia, Brazil

Fig: **5 : Levels of bypass**

Type of Load	Power Rating(W)	Quantity	Demand Factor	Actual Power(W)
Medium size Deep Freezer	130	1	0.5	65
Washing Machine	280	1	0.5	144
Microwave Oven	1000	1	0.5	500
Electric Pressing Iron	1000	1	0.5	500
Air-Conditional	1170	1	1.0	1170
Refrigerator	500	1	0.5	250
Ceiling fan	100	5	0.7	350
Incandescent Bulb	60	23	0.7	966
Sony 21" Television	100	1	0.5	50
Sharp 14" Television	80	1	0.5	40
Sony Music System	100	1	0.5	50
DSTV Receiver	50	1	0.5	25
DVD Player	50	1	0.5	25
			Total	4135

Load Assessment of the Customer's Three-Bedroom Apartment.

Table: 1.

MEASURES AND METHODS OF STEALING ELECTRICITY

In general, electricity consumers may be generalized as genuine customers, partial illegal consumers, and illegal consumers. There are several simple and sophisticated methods used in pilfering electricity, discusses factors that influence illegal consumers to steal electricity. The most common and simplest way of pilfering electricity is tapping energy directly from an overhead distribution feeder as shown in the diagram below. The next most prominent method of electricity theft is the manipulation of energy meters

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

that are used for recording and billing industrial, commercial and household energy consumption. Though there are many techniques for tampering with such meters, some of these may include:

- Exposing meters to strong magnetic fields to wipe out the memory.
- Inserting a film or depositing high viscous fluid to disturb the rotation of disc.
- Implementation of sophisticated technologies like remote sensing devices.
- Tampering the crystal frequency of integrated circuits.
- Creating a link between the breaking control wires in an energy meter would divert the current reading in the meter reflecting zero reading at all times.
- In the case of electronic meters, Radio Frequency (RF) devices are mounted to affect the accuracy of the meter.
- A shunt is installed between the incoming and outgoing meter terminals.
- Inter-changing the incoming and outgoing terminals of the meter.
- Damaging the pressure coil of the meter.
- Resetting the meter reading.
- Introducing unwanted harmonics.
- Exposing the meter to mechanical shock.
- Voltage is regulated from the meter terminals, making it read lesser quantity then the original consumption.

Figure 6: **Tapping electricity directly from a distribution feeder - bypassing the meter**.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Other engineered methods of tampering with the meter without damaging its terminals are illustrated below. Two-watt hour meters (employed for measuring the energy consumed by large loads with three phase electric supply) are tampered according to the following process: Damage the terminal seal; connect one of the load terminals to the ground; and open the ground wire from the energy meter. In the case of three phase meters, phases are shifted to lower the power consumption reading by the energy meter. Another popular way of lowering the energy meter reading without directly tampering with the meter is shown in Figure below. Here, supply voltage is regulated to manipulate the meter reading. Illegal consumers accomplish this by using one of the three phases; disconnect neutral from the distribution feeder, and using a separate neutral for the return path. Therefore, the energy meter assumes that the voltage between the connected phase and this new neutral is zero, implying that the total energy consumed is zero. Another way of stealing electricity is by isolating neutral and disturbing the electronic reference point by physically damaging the meter. The voltage to be read by energy meter can then be manipulated by controlling the neutral. In general, illegal consumption of electricity will be predominant only at desired hours of the day - when the customer's demand is high i.e. using legal electricity for small household loads and illegally tapped electricity for heavy loads. This kind of theft (partial illegal consumption) is very difficult to measure, as the energy consumption pattern is uneven over a period of time. In addition, corrupt employees are often responsible for billing irregularities; they record an amount of consumption that is lower than the original consumption. On the other hand, improper calibration and illegal de- calibration (during manufacturing) of energy meters can also cause NTL. In most of the meter tampered locations, damaged meter terminals and/or illegal practices may not be visible during inspection.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

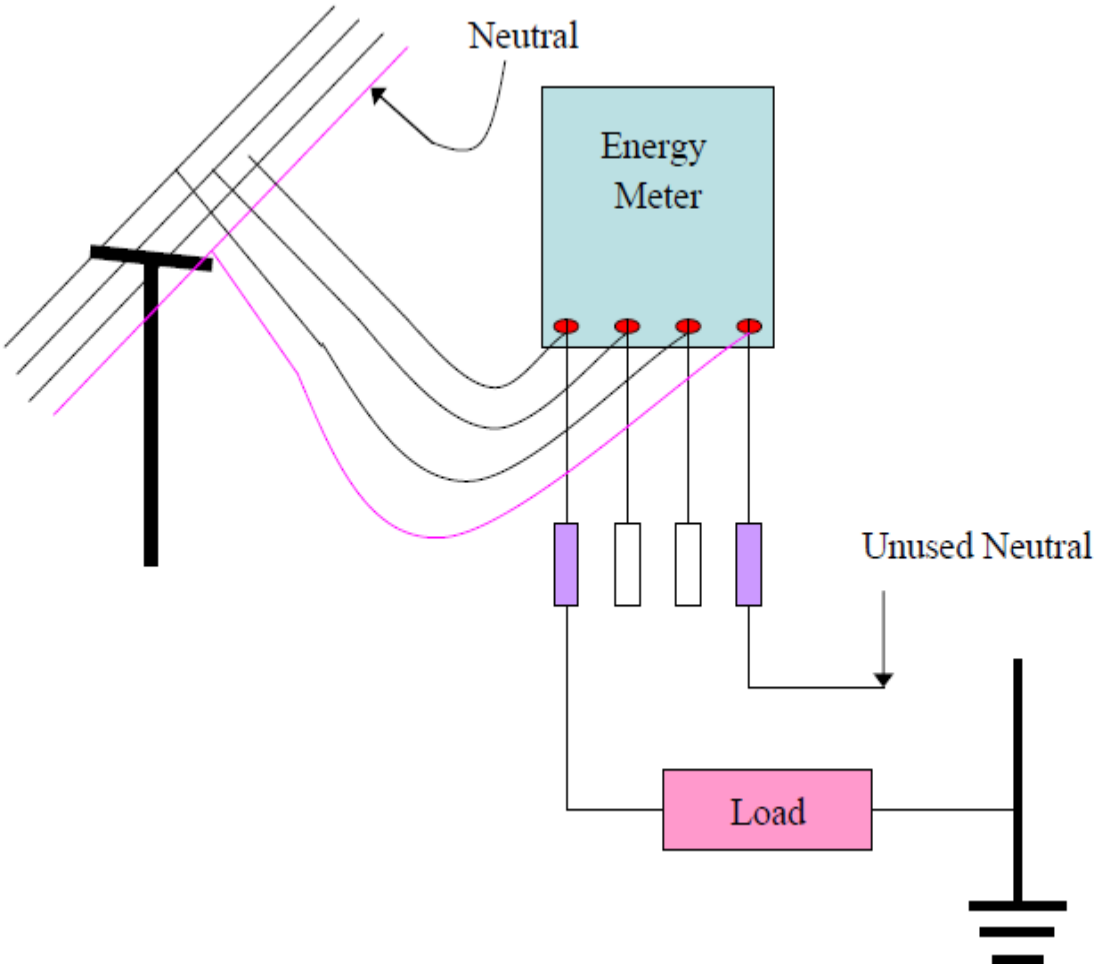


Figure 7: Technique used by illegal consumers to regulate the supply voltage and manipulate the energy meter reading

FACTORS THAT INFLUENCE ILLEGAL CONSUMERS

Factors that influence consumers to steal electricity depend upon various local parameters that fall into multiple categories like social, political, economic, literacy, law, managerial, infrastructural, and economical. Of these factors, socio-economic factors influence people to a greater extent in stealing electricity. More concisely, some of the important factors are:

- The belief that it is dishonest to steal something from a neighbor but not from a utility (public or large entity).
- Higher energy prices, unemployment or weak economic situation of a consumer.
- Corrupt employees of the utilities are responsible for billing irregularities. In some cases, total money spent on bribing utility employees is less than the money that would have been paid for consuming the same amount of electricity legally.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Some consumers might not be literate about the issues, laws and offenses related to the energy theft.
- Weak accountability and enforcement of law.
- Reasons to hide total energy consumption (e.g. Consumers who grow marijuana illegally or small-scale Industries to hide overall production/turnover).

In essence, electricity theft is proportional to the socio-economic conditions of the consumer.

DESIGN OF PREPAID ENERGY METER

The proposed idea is not to replace the existing energy meter and chalk out a completely new prepaid meter but up-grade the available energy meters to prepaid meters and Load meter. Thus, our design primarily has an energy meter, a prepaid card and the communication module encapsulated and provided as an upgrading attachment along with a contactor and a liquid crystal display (LCD).

Energy Meter*:* The electromechanical energy meter calculates the electrical energy or units consumed by the load based on the mechanical energy of the disk or rotor. The electronic meter has this existing structure attached with a microcontroller programmed to perform specific calculations and present it in terms of electrical energy units consumed to a prepaid card. The meter is also connected to a contactor apart from the consumer load.

Prepaid Card and Communication Module*:* The prepaid card is the most important addition to the design. The power utility sets the amount in the prepaid card to a measure that the consumer recharges the card to, called Fixed Amount. The tariff rates are already programmed and fed into the card. As the load is consumed, the meter sends the units consumed to the prepaid card which continuously converts these units into expenditure at each instant and then subtracts it from the fixed amount. The communication module uses mobile communication to share prepaid card balance with power utility at certain instants as required by utility for tracking the balance and also for any other application e.g. Demand Side Management (DMS) etc. The fixed amount in the prepaid card will go to zero eventually with the consumption. The consumer can recharge the prepaid card by prepayment through internet. The utility on receipt of recharge request and desired prepaid amount, recharges the customer's energy meter i.e. prepaid card. The prepaid card sends a signal to the contactor for monitoring the supply to the consumer. The communication module has prepaid card encapsulated inside the encryption authentication module which is Embedded Security Access Module (ESAM). It thus enables the card to use the mobile communication to communicate with power utility and share information regarding the card's balance details.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Contractor*:* A local contractor is the connecting link between the consumer load and utility supply. The opening and closing of this contactor depends on the balance present in the prepaid card at a moment. While the prepaid card has some fixed amount more than zero, it stays closed and keeps the utility supply uninterrupted to the consumer load. When the card runs out of balance, it opens and disconnects the load from the supply. Hence, even when the energy meter receives voltage supply, it does not reach the load while the contactor is open because the balance in the prepaid card is not available. Since the contactor too will consume some amount of electrical energy, it will be inclusive in the calculations made by meter and prepaid card.

Power line for Load meter.

AMR is a method where electronic data is transmitted over power lines back to the substation, then relayed to a central computer in the utility's main office. This would be considered a type of fixed network system the network being the distribution network which the utility has built and maintains to deliver electric power. Such systems are primarily used for electric meter reading. Some providers have interfaced gas and water meters to feed into a PLC type system. Some technology like the touch technology, handheld technology are not common in Nigeria but the only technology to be used is the mobile technology, because the meter readers still have to go to the houses, offices and other places where the meters are placed. In addition to the mobile technology, we need extra devices which are not very expensive. The Power Line technology is not also feasible for Nigeria perspective. In Nigeria high voltages transmits through the power line cable. As the voltage is high so the transmitted data will be corrupted by the attenuation. All the power line cable of our country is not placed under the ground. It is situated in the open air. So the cable faces different environmental problems. So the actual data may not transmit to the provider end. As a result this technology is also not feasible in our country. The fixed RF technology has small coverage area. As a result, this method consist of a number of series of antennas, towers, collectors, repeaters, or other permanently installed infrastructure to collect transmissions of meter readings from AMR capable meters. So this is not cost efficient for the customers. The main reason is to introduce an AMR system which is cost efficient, to overcome the problem of bypassing, to issue that the prepaid meter reading is the same with the Load meter, improve meter reading accuracy, to enable faster, more efficient reading times and billing process, Significantly increase operational efficiency by providing real time pricing and time-of-use metering.

EXPERIMENTS AND FINDINGS

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Almost all the meter reading systems consists of three primary components. We divided the whole AMR system into four basic units. These are: Reading unit, Communication unit, Data receiving and processing unit, billing system.

Fig: 8 Component of Meter Reading.

Reading unit

In this part basically two important jobs have been done. At first the analog meter reading was converted to digital bits sequence (0 or 1). After that the data are available in the microcontroller for transmission. First challenge is how we can get reading automatically from analog digital watt meter. It was analyzed that the rotations of the disk of the meter are needed to be counted. If it is possible to measure the number of rotation of the disk of the meter then the meter reading can be calculated. There are various types of sensors that are available to perform the reading of the meter. Infrared can be used as a sensor. The infrared transmitter generates frequency and the receiver receives it. If there is no obstacle between the infrared transmitter and the infrared receiver than the infrared receiver give one value. But if there is any obstacle then the receiver gives another value. So this event can be used to count the rotation of the disk. The infrared transmitter and receiver have to place in such a way so that when the disk of the meter rotates it can be recognize without any obstacle.

COMMUNICATION TECHNOLOGIES

Utilization of the smart meter system involves a large quantity of data transfer between the utility, smart meter, and home appliances in the network. This data is sensitive, confidential, and access to this data should be given to only a few personnel. With the restrictions on this data, security guidelines are formulated for transmission, collection, storage, and maintenance of the energy consumption data. The communication standards and guidelines were formulated to ensure that data transfer within the network is secure. It is equally important that this data must represent the complete information regarding the customer's energy consumption and status of the grids without any potential manipulations or miscalculations. So, this data must be authenticated and should reflect information about the target devices correctly. In the figure below, devices in the transmission sector ensure proper transmission of generated energy, control systems in the distribution sector ensure monitoring and controlling of faults, communication devices like protocol gateways, data collectors, repeaters and network operations coordinate data as well as control signals between all the devices in the communication network.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The common network selected has to support the required operation of the smart meter system even on power outage and support distribution automation. In addition, the selected network and its components must be cost effective and must support "traffic prioritization" i.e. they must prioritize the delivery of data based on its time and direction sequence. Communication technology to be chosen should be cost effective, provide good transmission range, better security features, bandwidth, and power quality with least possibility of repetitions

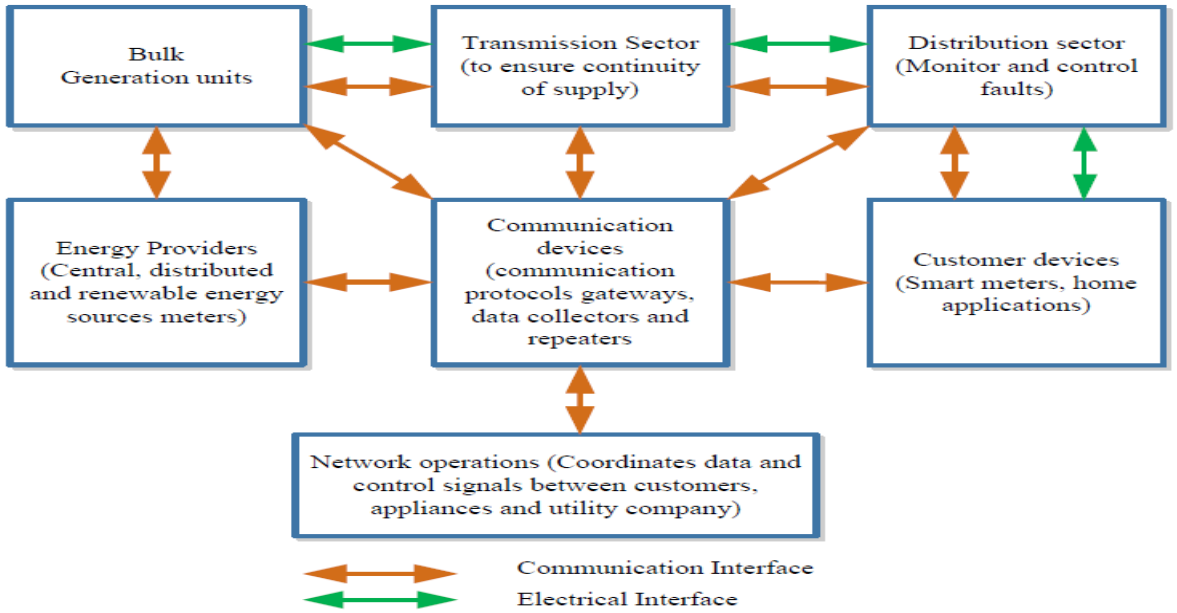


Figure 9: Framework of communication and electricity networks in a smart grid environment.

Bluetooth technology can be a possible option for communication of control signals and transmission of energy consumption data. In view of implementing this technique, B.S. Koay *et al.* proposed a Bluetooth based energy meter that can collect and transmit the energy consumption data wirelessly to a central base station. Power Line Communication (PLC) and Broadband over Power Line (BPL) communication are the other possible options of data transfer supporting the higher level communication suites such as TCP/IP. PLC uses the existing electricity grid, cellular/pager network, and mesh network, a combination of licensed and unlicensed radios, wireless modems, existing internet connections, power line communications, Wi-Fi, WiMAX, and Ethernet with a protocol to upload data using IEC DNP. PLC technology effectively automates the process of data collection in smart meter applications. Despite huge overhead due to IPv6, IPv6 can be applied to physical layer with lower data rates. However, IPv6 combined with Media Access Control (MAC) algorithm accomplishes less delay time and higher throughput. Though this combination might slightly reduce the usable data transfer rate, it will not affect the overhead at the MAC layer. IP based network protocol could be another promising option for communication because of its advantages over other technologies while satisfying the security standards of the smart grid communications. In addition, TCP/IP forms an efficient communication platform across

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

multiple devices. In addition, Session Initiation Protocol (SIP), a text-based signaling protocol, is employed for controlling multimedia sessions like video and Voice over Internet Protocol (VoIP). SIP integrates several features of HTTP and Simple Mail Transfer Protocol (SMTP). SIP is an open and standards-based technology, which provides a robust communication medium for the smart grid applications. SIP can be implemented on top of TCP, User Datagram Protocol (UDP), or Stream Control Transmission Protocol (SCTP). A new architecture based on DNP3 is proposed by T. Mander *et* al. DNP3 produces a protocol discontinuity between DNP3 devices (used for regulated power 20 system operations) and TCP/IP devices (used for the smart load and demand management). The advantage with this architecture is, the discontinuity limits the vulnerable attacks from other TCP/IP devices. Some security enhancements such as data object security and a security layer may be added to DNP3, as this protocol by itself is not adequately safe for collaborative operations. Data object security appends additional rules to access data thereby preventing the unauthorized access that can potentially manipulate data and device operations. An energy meter based on Peer-to-Peer (P2P) network is presented in S. Rusitschka *et al*. The utilization of P2P network enhances the range of operations. In addition, several value added services can be employed. P2P communication uses the internet, which leads to a cost effective design of smart grid communication networks. In addition, the P2P network utilizes the resources of participating homes optimally.

Yet another network, Zigbee, is a potential communication network for transfer of data as well as control signals. As many industrial and household entities maintain a computer with 802.11.x, Zigbee protocol can be used with Home Area Networks (HANs) for data transfer over 802.11.x. This technology can be used instead of increasing the operating clock frequency in the crypto core in order to reduce the response time and verification delay; J. Kim *et al.* proposed the mode toggling approach on the design process for AES-CCM module. They have also adopted the optimal security material management module. These design methodologies and the obtained response time allow the cryptographic core to maintain the minimum clock frequency, while staying within the constraints, ensuring the reduction in total dynamic power consumption.

General Packet Radio Service (GPRS) technology is another potential communication medium for transferring both the data and control signals wirelessly over long distances. In contrast to other communication network technologies, only a few communication characteristics that represent GPRS communication network have been assessed. That being said, lack of tools for detecting a network failure would be a major setback in implementing GPRS network in many geographical locations. Before deploying a GPRS based communication system in a specific location, availability and quality of the signal has to be determined. Parallel processing and implementation of the Field-Programmable Gate

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Array (FPGA) hardware can reduce the time elapsed for interpreting the data and obtaining the status of the distribution network. Adoption of reconfigurable logic for processing of data minimizes the amount of data to be generated by a Smart Meter.

This is one of the most important and challenging part of this system. This part is challenging in the sense, that data is the most valuable part for meter reading and billing system. Data should be transmitted in an efficient manner without any loss of data. Let's describe about this challenging part. From the above description it is clear that digital data is always ready for transmission. Meter reading are stored in Microcontroller's EPROM and this data is always ready for transmission. But the main concern was how data can be transmitted efficiently? From the background study it is realized that all the existing communication units are not feasible for higher cost and infrastructure of Nigeria Power Supply. After studying different technologies, Wimax has been chosen for communication. In Wimax possibilities of data corrupting is very less and the coverage area is very high in Wimax when compare to other communication facilities. For the purpose of communication between meter end and the server end, a small miniature and low cost Wimax Transceiver module is required in each meter and in the server end. A transceiver module is a module which can transmit and receive data at a time. After searching a miniature and low cost transceiver module has been found.

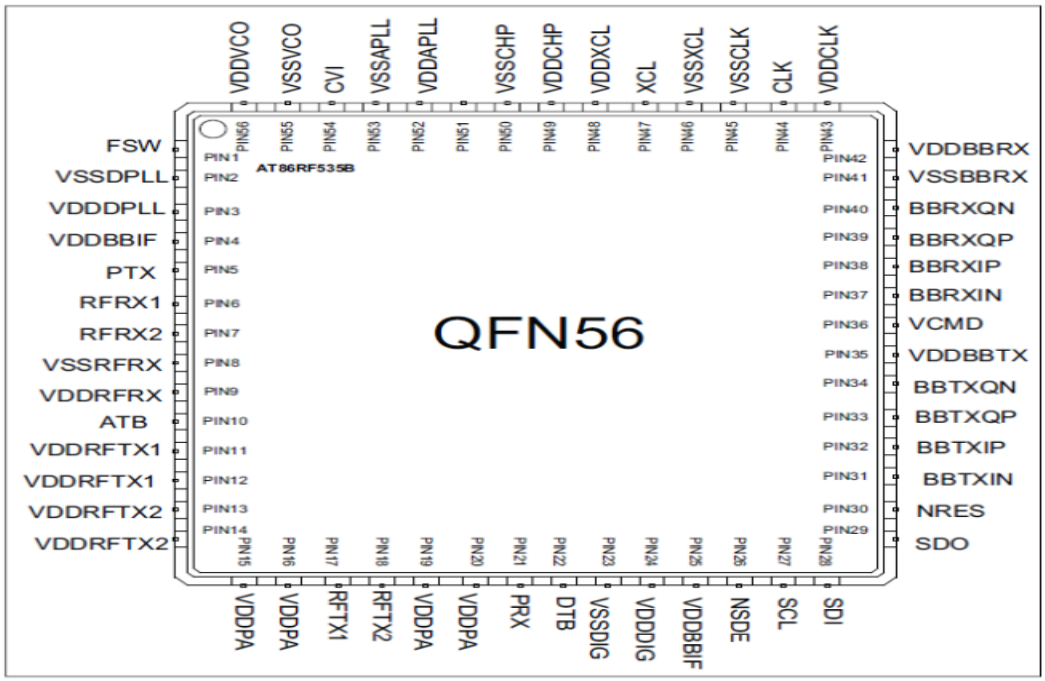


Fig. 10. Pin Information of AT86RF525B.

The model name is AT86RF535B. AT86RF535B is a fully integrated, low cost RF 3.5GHz Low-IF/Zero-IF conversion transceiver for WiMAX applications. It combines excellent RF performance, small

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

size, and low current consumption. The AT86RF535 chip is fabricated on the advanced SiGe BiCMOS process AT46000. The transceiver combines LNA, PA driver, RX/TX mixer, RX/TX filters, VCO, Synthesizer, RX Gain control, and TX Power control, all fully digitally controlled. This transceiver module is miniature in size. This Wimax transceiver module can be set up inside of the current analog wattmeter. And this transceiver also cost very lower than other transceiver. In the server end there will be a transceiver and each meter will contain a miniature transceiver. A computer application will run at the server end which can send an address of a particular meter to the microcontroller and the microcontroller will supply the address to the transceiver. Then the transceiver will send the address to all meters. Generally all the transceiver of the meters will be in sleep mode. When a transceiver of the meter receives the address sent by the server transceiver then it compares that is the request is for itself or not. If the request is for itself then it give a high signal to the microcontroller and the microcontroller send the data to the transceiver. After getting the data from the microcontroller the transceiver transmit the data. The server end transceiver receives the data and provides the data to the server end microcontroller. The microcontroller sends the data to the computer. This is the overall communication part of our system. Fig. 6 shows the data flow in communication unit of our proposed system

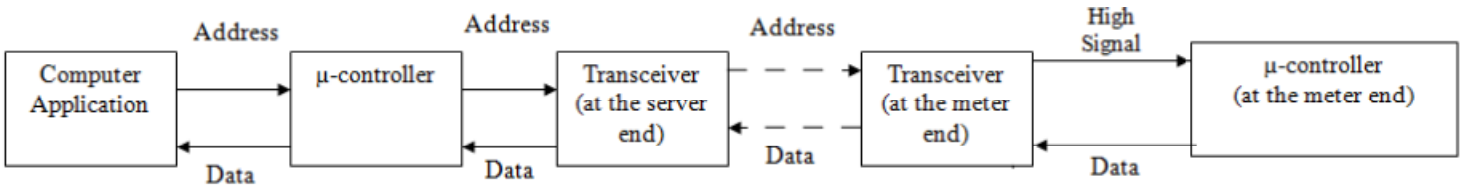


Fig: 11 .Data flow in the communication units.

Data receiving and processing unit

This is the third part of the proposed AMR system. In this part the received data is processed by the system for future purpose. For data processing purpose a computer application has been developed. The task of the application was to take a meter number form the user and give the address to the microcontroller through serial port. Then the microcontroller does the communication task. After communication part the microcontroller get the data form transceiver and the meter reading is available in the server end microcontroller. Then the data is sent to the computer and the computer application receives the data from the microcontroller. This data can be stored in the database and can be displayed to the requested user.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

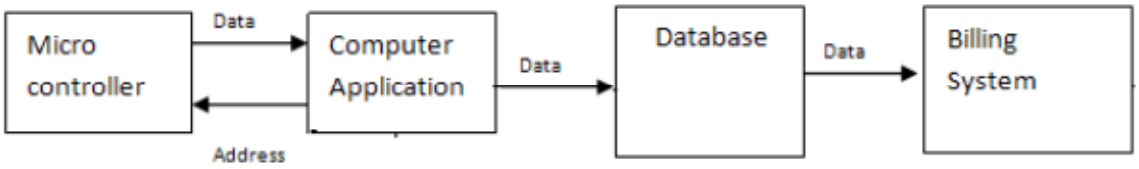


Fig: 12 Block diagram of data receiving and processing unit.

Billing System

The billing system has been developed in our system which can take the meter number and can generate bill for that meter. It uses the data of the database those are collected from the meter reading through all the unit of our system. This system also can be used for analysis on electricity usage for each meter.

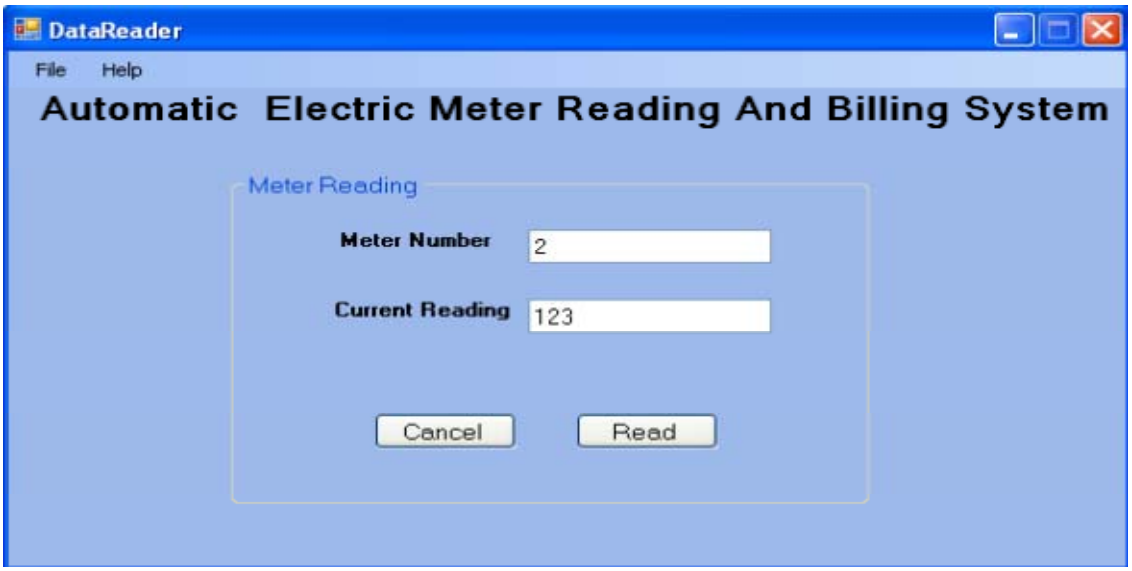


Fig 13 : Example on demand Reading using the computer application.

Overall Conceptual design

In this system the existing analog meter will be used and our proposed miniature module will be added to each meter. A module will be situated in the server end and this module will be connected with the server computer. The entire module will be connected through Wi-Max technology. The overall conceptual design has given in fig. 9.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

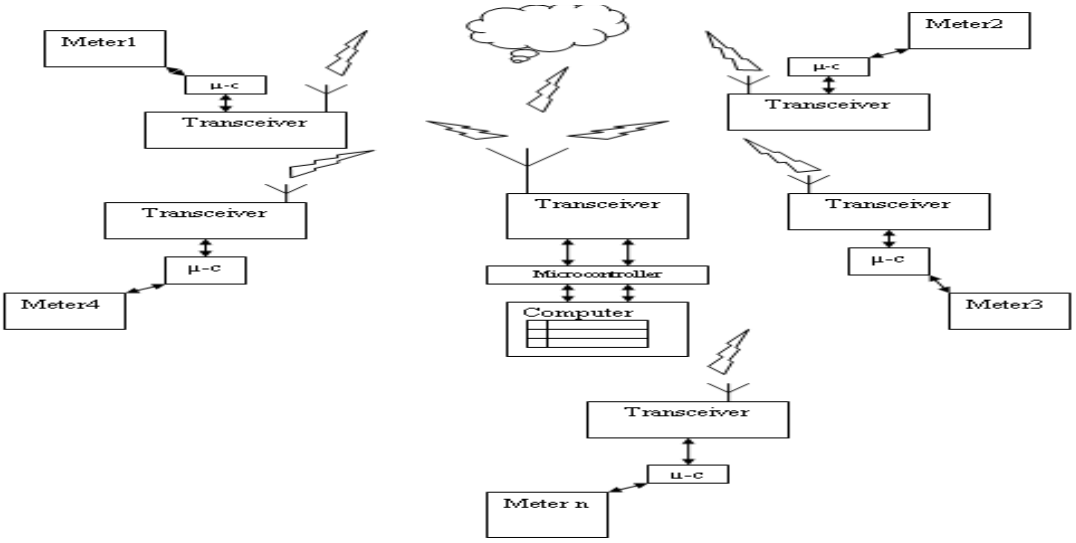


Fig: 14. Conceptual Diagram of our proposed AMR.

WIMAX AS A TRANSMISSION MEDIA

WiMAX, the Worldwide Interoperability for Microwave Access, is a telecommunications technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access. It is based on the IEEE 802.16 standard, which is also called Wireless MAN. The name WiMAX was created by the WiMAX Forum, which was formed in June 2001 to promote conformance and interoperability of the standard (http://en.wikipedia.org/wiki/WiMAX). WiMAX has a theoretical maximum bandwidth of 75Mbps. This bandwidth can be achieved using 64QAM 3/4 modulation. 64QAM can only be utilized under optimal transmission conditions. WiMAX supports the use of a wide range of modulation algorithms to enable the most bandwidth to be realized under all conditions (http://en.wikipedia.org/wiki/WiMAX). WiMAX has a theoretical maximum range of 31 miles with a direct line of sight. Near-line-of-sight (NLOS) conditions will seriously limit the potential range. In addition, some of the frequencies utilized by WiMAX are subject to interference from rainfade. The unlicensed WiMAX frequencies are subject to RF interference from competing technologies and competing WiMAX networks. WiMAX can be used for wireless networking in much the same way as the more common WiFi protocol. WiMAX is a second-generation protocol that allows for more efficient bandwidth use, interference avoidance, and is intended to allow higher data rates over longer distances.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

ONLINE FEEDBACK

Web-based applications for customer feedback are favoured by utilities. They are relatively inexpensive (no costs sunk in the manufacture and distribution of dedicated displays), can be updated rapidly, and ensure that the supplier has access to, and controls all the information. They can also be used to process data for sending to customers via a range of devices, including mobile phones and personal computers. This could be a promising application for alerting householders to abnormal consumption. Web applications can show householders a great deal of detail over time about their own consumption and about the wider picture: how their usage compares with that of others; or what the demand curve for the nation or region looks like (at times of supply constraint). The recent move by Google into providing energy feedback demonstrates interest from third parties in providing this particular form of energy service. However, there are limitations, chief among them the difficulty of getting people engaged deeply enough to access the information on a regular basis. It takes extra effort and determination to look up consumption data online compared with the effort needed to check a dedicated display in the home. The UK government response to the latest consultation on smart metering comments that: The Government's position remains that a standalone display should be provided with the smart meter. The provision of a display is important to securing the consumer benefits of smart metering, delivering real time information to consumers on their energy consumption in a readily accessible form. Whilst, there are alternative means of information provision evidence to date suggests they may often be less effective, especially where they require positive action by the consumer to access information. Experience in the USA and Sweden has, for example, shown that where smart meter data has been available online, the usage rate has been low at 2 to 4 per cent of customers. (DECC, 2009b)

The possibilities for online feedback are evolving, along with support services and customer-relations programmes. Some are proving successful in terms of engagement, but again it needs saying that they do not necessarily need smart meters for this: people can key in their meter readings over a period of time in conjunction with a feedback or advice programme, and there are successful examples of this.

This overview of feedback arrangements shows something of what has been achieved in terms of customer engagement without smart metering. It also points towards what could be achieved through a well-designed 'smarting' of metering systems, i.e. a system designed with customer relations and customer learning as priorities. Information on its own may or may not be of any practical use to consumers; it has to be absorbed and tested in particular buildings, in company with particular people, and in particular climatic, regulatory, and political circumstances. Smart metering can greatly improve the information available to both supplier and consumer; however, the challenge is to develop

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

communications that can be used to select the most useful information for the consumer and to combine them with advice and other pointers to enable effective action.

METHODOLOGY

In this section, the overall design of the system is discussed in terms of three-tier architecture. Three tier architectures are variations of the well-known client/server computing model. The model was proposed as an alternative to centralized mainframe and time sharing computing. In this model, the client interacts with the user possibly via a GUI interface, and requests on-line services from the server. The server, on the other hand, answers these requests and provides the services. The fact that this system is spread across more than two different entities suggests three-tier architecture. Such architecture brings clear logical structure to the system. A major advantage of the three-tier architecture is scalability, that is it supports hundreds of users and able to manage these connections (via queuing, for example) better due to the middle tier. Scalability is a major requirement for our design since there could be thousands of customers who are trying to update the balance on their prepaid electricity card and trying to establish a session with the servers.

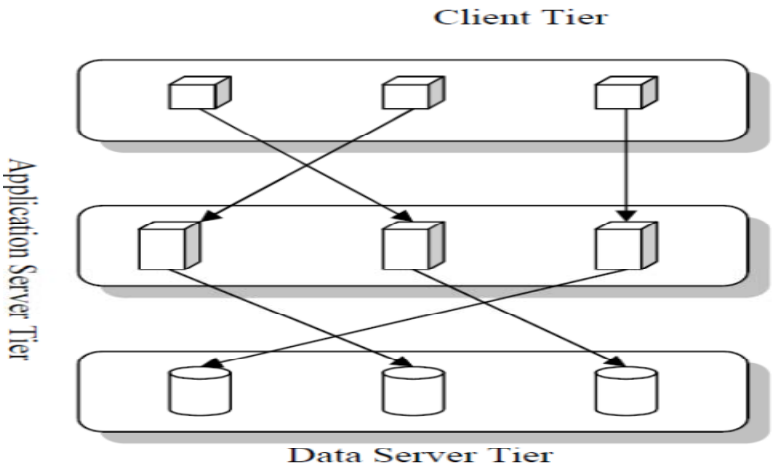


Figure 15: Three Tier architecture.

In additions, with the three-tier architecture most of the application (business) logic like locating the appropriate database, checking authority, generating query, is moved to the middle tier. Therefore, in the case of the three-tier architecture, changes in the business logic result in less client tier changes. Another advantage of the three-tier architecture is that its data security is increased because the client tier no longer can access the data directly; it has to go through the middle tier first.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

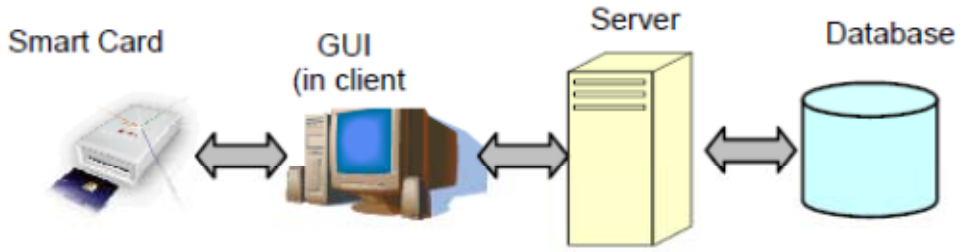


Figure 16. Block diagram of customer and utility processes

A customer purchases electricity credit at the nearest electricity POS. The electricity POS device is commonly referred to as a credit dispensing unit (CDU). Electricity is purchased as a monetary value and encoded as a kilowatt hour (kWh) value in the token. The encrypted credit transfer token is generated by the CDU and printed on a receipt or encoded on a magnetic card, depending on the meter type. The meter's credit register is only updated once the token has been correctly decrypted and accepted by the customer's meter. A prepayment token is requested from a Server that is remote from the actual point of sale client application making the request. The token is only generated on the Server and transferred to the POS client, once the transaction, the POS client and the payment mechanism has been authenticated and authorized. The connection between the POS client and the Server is a standard computer network communications channel (dial-up, Internet, frame-relay, and General Packet Radio Service, or WIMAX). Diagram is illustrated in fig below.

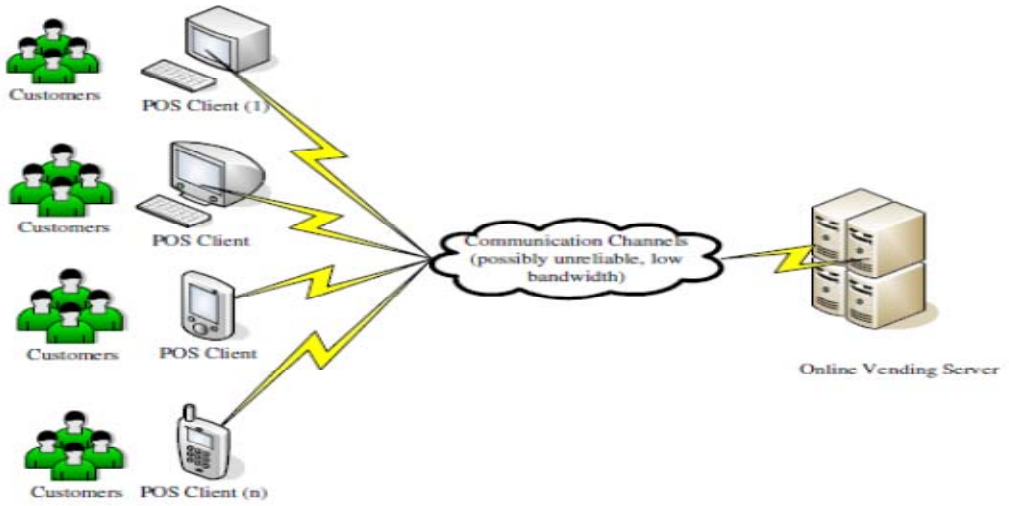


Figure: 17. The online vending context.

The POS clients must communicate with the online vending server to complete a prepaid vending transaction. Without such a communications link no prepaid transactions are possible. The prepaid card is the most important addition to the design. The power utility sets the amount in the prepaid card to a measure that the consumer recharges the card to, called Fixed Amount. The tariff rates are already

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

programmed and fed into the card. As the load is consumed, the meter sends the units consumed to the prepaid card which continuously converts these units into expenditure at each instant and then subtracts it from the fixed amount. The communication module uses mobile communication to share prepaid card balance with power utility at certain instants as required by utility for tracking the balance and also for any other application e.g. Demand Side Management (DMS) etc. The fixed amount in the prepaid card will go to zero eventually with the consumption. The consumer can recharge the prepaid card by prepayment through internet. The utility on receipt of recharge request and desired prepaid amount, recharges the customer's energy meter i.e. prepaid card. The prepaid card sends a signal to the contactor for monitoring the supply to the consumer. The communication module has prepaid card encapsulated inside the encryption authentication module which is Embedded Security Access Module (ESAM). It thus enables the card to use the mobile communication to communicate with power utility and share information regarding the card's balance details.

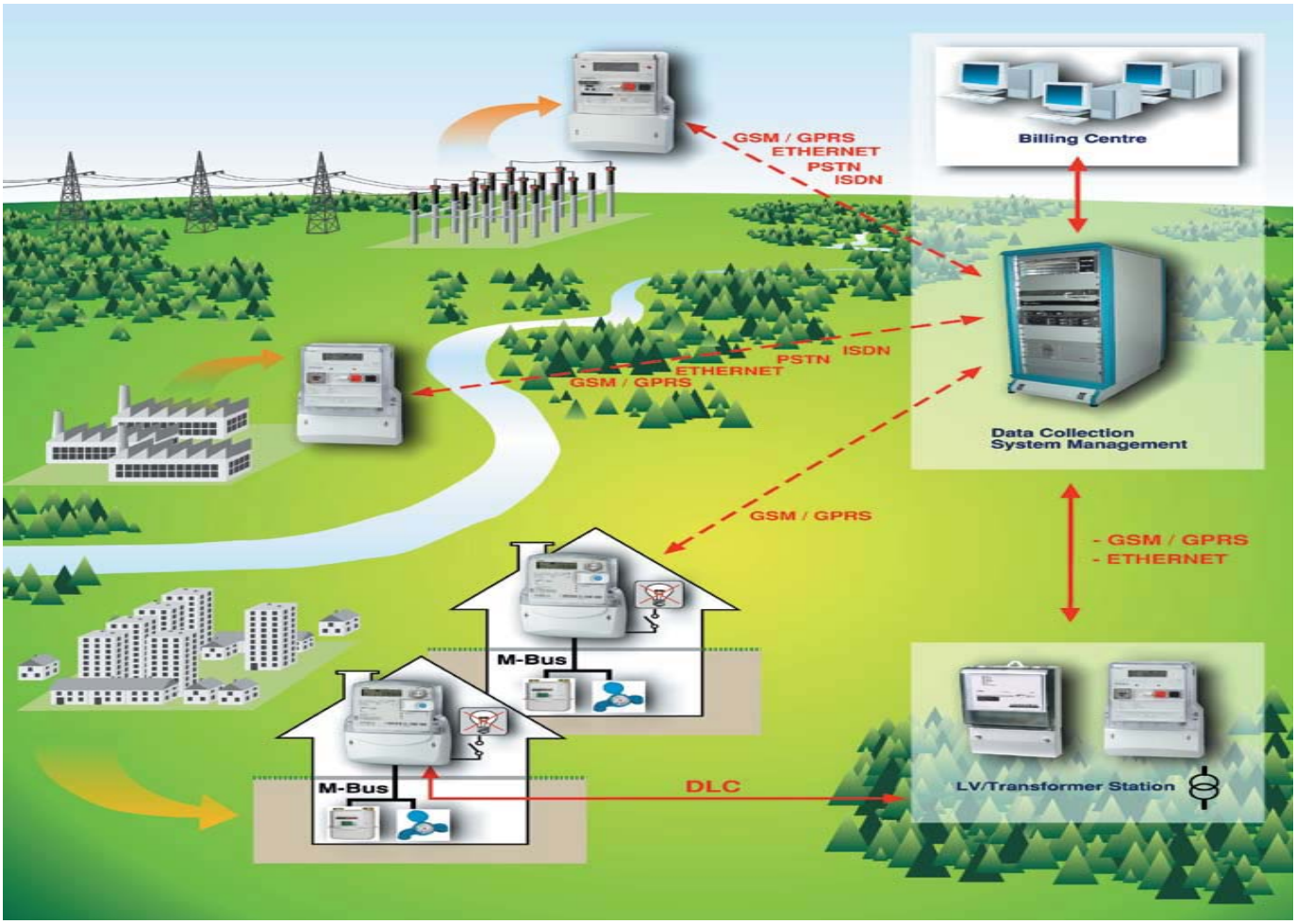


Figure 18: Main components of the smart card system

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

CONCLUSSION

Today, a high percentage of electricity revenue is lost to power theft, incorrect meter reading and billing, and reluctance of consumers towards paying electricity bills on time based on postpaid meter. Considerable amount of revenue losses can be reduced by using Prepaid Energy Meters. A prepaid energy meter enables power utilities to collect energy bills from the consumers prior to the usage of power by delivering only as much as what has been paid for. This research provides a prepaid energy meter behaving like a prepaid mobile phone. The meter contains a prepaid card similar to mobile SIM card. The prepaid card communicates with the power utility using mobile communication infrastructure, once the prepaid card is out of balance, the consumer load is disconnected from the utility supply by the contactor. The IP-based controller for the prepaid meter and Load meter is to provide a simple way of detecting electricity power theft without any human intervention. The Load meter would indicate exact building or location and distribution line on which unauthorized taping is done in real time. It would be time saving if distribution company personnel take reading by this wireless technique and also it would provide a digital record in case of any judicial dispute which will be use for comparative analysis between the prepaid meter. The idea is to maximize the profit margin of power utility company, efficient online control of the total amount of electricity consumed in a specific location and be able to detect when there is bypass by the user either by shoot- hunting without connecting the cable through the digital meter or parts of the equipment are connected through to the smart meter why high voltage equipment are bypassed.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

REFERENCES

[1]. Oseni, T. 2002. "Obasanjo Laments NEPA's Inefficiency". *Nigerian Tribune*. 16 July 2002.

[2]. Ogujor, E.A. 2007. "Reliability Assessment of Electric Power Distribution: A Case Study of 2 x 15MVA, 33/11kV Ugbowo Injection Substation". Ph.D. Thesis. University of Benin: Benin City. Nigeria.

[3]. Ogujor, E.A. and Kuale, P.A. 2007. "Reliability-Based Electricity Billing System". *Journal of Electrical/Electronic Engineering*. 11(1):22-29.

[4]. Annon, O. 2001. "Management Introduces RCM Project". *NEPA Review*. (July-Sept, 2001):6.

[5]. Customer's Post-Paid Electricity Bills between 15 January, 2007 and 15 January, 2008. (Name withheld for privacy)

[6]. K. van den Berg, "Development of on-line vending standards," South African Prepayment Week, Johannesburg, South Africa, 2003.

[7]"Prepayment Frequently Asked Questions,"Eskom,http://www.eskom.co.za/live/content.php?Item_ID=591. Last accessed on 21 September 2006.

[8]. K.P. Subramoney, Online Vending - Industry trends towards an industry specification, Eskom Resources and Strategy, Research Report, RES/RR/01/15519, 2002.

[9]. P. Johnson, "The Standard Transfer Specification – Past, Present and Future," Eskom, Internal Document, 2002.

[10]. K.P. Subramoney, Development of a prepaid Online Vending Interface Specification (Another world first for the South African Prepayment Industry), Energize (Power Journal of the South African Institute of Electrical Engineers), March 2004.

[11]. B. Meyer, S. Moodley, Prepayment Evolution – Key Features of a Proven Revenue Management System, ESI Africa (The Power Journal of Africa), Issue 1, 2005, pp. 12-13.

[12]. Dr. Mohd Yunus B Nayan1, Aryo Handoko Primicanta 2009. Hybrid System Automatic Meter Reading. International Conference on computer technology and Development,(ICCTD -09), pp: 264-267.

[13]. Kwang-il Hwang 2009. Fault-tolerant ZigBee-based Automatic Meter Reading Infrastructure. Journal of Information Processing Systems, Vol.5, No.4, pp:221-228.

[14]. H.G.Rodney, Tan IEEE, C.H.Lee and V.H.Mok, 2007. Automatic Power Meter Reading system using GSM Network. The 8th International Power Engineering Conference, pp: 465-469.

[15]. Huibin sui, Honghong Wang, Ming-Shun Lu and Wei-Jen Lee 2009. An AMI System for the Deregulated electricity Markets. IEEE Transaction on Industry Application, pp: 1-5.

[16]. Liting Cao Jingwen Tian Yanxia Liu 2008. Remote Wireless Automatic Meter Reading System Based on Wireless Mess Networks and Embedded Technology. Fifth IEEE International Symposium on Embedded Computing, pp: 192-197.

[17]. Bharath P, Ananth N, Vijetha S, Jyothi Prakash K. V. 2008. Wireless Automated Digital Energy Meter . IEEE International Conference on Sustainable Energy Technologies, pp: 564-567.

[18]. Li Xiaoguang Hu, "Design of an ARM-Based Power Meter Having WIFI Wireless Communication Module" IEEE 2009.

[19]. B. S. Koay, etc, "Design and implementation of Bluetooth energy meter", Proceedings of the Joint Conference of the Fourth International Conferee

IJCSIS AUTHORS' & REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore,Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Mrs Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Mr. P. Vasant, University Technology Petronas, Malaysia
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Mr. Praveen Ranjan Srivastava, BITS PILANI, India
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Mr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Mr. Tirthankar Gayen, IIT Kharagpur, India
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

CALL FOR PAPERS
International Journal of Computer Science and Information Security

IJCSIS 2014
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on
its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embeded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcsis/authors-notes .

ISSN 1947 5500
http://sites.google.com/site/ijcsis/